

RIVISTA ELETTRONICA DI DIRITTO, ECONOMIA, MANAGEMENT



Inquadra il QR-CODE
per il download
degli altri numeri
della Rivista

Numero 1 - 2023

I professionisti della custodia dei contenuti digitali

A cura di Andrea Lisi

FONDATA E DIRETTA DA
DONATO A. LIMONE

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente, che ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla trasformazione digitale, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo nei settori pubblico e privato.

La rivista ha anche la finalità di ospitare contributi di giovani studiosi per valorizzarne le attitudini alla ricerca e il loro contributo allo sviluppo delle scienze giuridiche, sociali, economiche e manageriali.

Direttore responsabile: Donato A. Limone

Comitato scientifico: Estanislao Arana García, Catedrático de Derecho administrativo de la Universidad de Granada (Spagna); Piero Bergamini (Comitato Direttivo del Club degli Investitori di Torino); Francesco Capriglione (professore di diritto degli intermediari e dei mercati finanziari, Luiss, Roma); Mario Carta (Professore di diritto dell'Unione europea dell'Università degli Studi di Roma Unitelma Sapienza); Enzo Chillelli (esperto di sanità e di informatica pubblica); Claudio Clemente (Banca d'Italia); Fabrizio D'Ascenzo (professore ordinario, preside della Facoltà di Economia, Università "La Sapienza"); Angelo Del Favero ("Health and Welfare School", Università degli Studi di Roma "Unitelma Sapienza"); Luigi Di Viggiano (Università del Salento; esperto di scienza dell'amministrazione digitale); Jorge Eduardo Douglas Price, ordinario di Teoria generale del diritto; Direttore del Centro di Studi Istituzionali Patagónico (CEIP), Facoltà di Giurisprudenza e Scienze Sociali dell'Università Nazionale di Comahue (Argentina); Maria Rita Fiasco (consulente, Vice Presidente Assinform); Donato A. Limone (professore di informatica giuridica, fondatore e direttore della "Rivista elettronica di diritto, economia, management"); Andrea Lisi (Avvocato, docente ed esperto di Diritto dell'Informatica; Presidente di Anorc Professioni); Valerio Maio (ordinario di diritto del lavoro, Università degli Studi di Roma, Unitelma Sapienza); Vincenzo Mongillo (ordinario di diritto penale, Università degli studi di Roma, Unitelma Sapienza); Mario Nobile (dirigente generale, responsabile della transizione digitale, Ministero delle infrastrutture e dei trasporti); Roberto Pasca di Magliano (Professore di Economia e gestione dell'Innovazione; Direttore School of Financial Cooperation and Development, Unitelma Sapienza); Gianni Penzo Doria (dirigente universitario di ruolo, direttore dell'Archivio di Stato di Venezia e dell'annessa Scuola di archivistica, paleografia e diplomatica); Pier Luigi Petrillo (ordinario di diritto pubblico comparato, Università degli studi di Roma, Unitelma Sapienza); Nadezhda Nicolaevna Pokrovskaja, docente universitario presso Herzen State Pedagogical University of Russia e Peter the Great Saint-Petersburg Polytechnic University; Francesco Riccobono (ordinario di teoria generale del diritto, Università Federico II, Napoli); Sergio Sciarelli (professore di economia aziendale, Università Federico II, Napoli); Marco Sepe (ordinario di diritto dell'economia, Università degli studi di Roma, Unitelma Sapienza).

Comitato di redazione: Alberto Bruni, Angelo Cappelli, Luca Caputo, Claudia Ciampi, Ersilia Crobe, Tiziana Croce, Wanda D'Avanzo, Sandro Di Minco, Paola Di Salvatore, Massimo Farina, Santo Gaetano, Paolo Galdieri, Salvatore Gallo, Fabio Garzia, Edoardo Limone, Emanuele Limone, Lucio Lussi, Marco Mancarella, Antonio Marrone, Alessio Mauro, Alberto Naticchioni, Cristina Evangelina Papadimitriou, Giulio Pascali, Gianpasquale Preite, Azzurra Rinaldi, Fabio Saponaro, Pasquale Sarnacchiaro, Sara Sergio, Franco Sciarretta.

Direzione e redazione: Via Riccardo Grazioli Lante, 15 – 00195 Roma - donato.limone@gmail.com

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno XIII, n. 1/2023

ISSN 2039-4926

Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010

Editor ClioEdu

Roma - Lecce

Tutti i diritti riservati.

È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte. La rivista è fruibile dal sito www.clioedu.it gratuitamente.

Codice etico: www.clioedu.it/rivistaelettronica#codice-etico

Procedure di referaggio: www.clioedu.it/rivistaelettronica#referaggio

Elenco dei numeri pubblicati: www.clioedu.it/rivistaelettronica

INDICE

Editoriale	
<i>Donato A. Limone</i>	3

Presentazione	
La costruzione di competenze interdisciplinari come presupposto indispensabile per la crescita digitale del Paese.	
<i>Andrea Lisi</i>	4

La custodia del patrimonio informativo pubblico: un'indagine a cura di ANORC	
<i>Alessandro Selam</i>	17

Il Responsabile della conservazione dei documenti informatici: intervista con l'A.I.	
<i>Luigi Foglia</i>	23

Il ruolo del Responsabile della transizione digitale nella progettazione di servizi on line	
<i>Sarah Ungaro</i>	29

Sezione I – L'evoluzione digitale degli archivi

Il ruolo della conservazione nel processo di digitalizzazione del Paese	
<i>Patrizia Gentili</i>	36

Gli archivisti e la conservazione degli archivi digitali	
<i>Micaela Procaccia</i>	43

Esisterà una gestione documentale nel 2026?	
<i>Andrea Piccoli</i>	49

Gli archivi digitali e l'art. 2086 c.c.: una risposta al principio di adeguatezza della struttura	
<i>Giuseppe Vitrani</i>	59

Strategie e buone pratiche per la selezione dei documenti informatici: sottofascicoli, sfoltimento e campionatura <i>Dimitri Brunetti</i>	64
---	----

Conservazione digitale: obiettivi e funzione archivistica <i>Gabriele Bezzi</i>	72
--	----

Sezione II - La custodia dei dati

Custodire dati ovvero storia di una migrazione <i>Monica Del Rio</i>	92
---	----

La custodia dei contenuti nella società dell'informazione: osservazioni sulla sentenza CGUE c-460/20 <i>Enrico Pelino</i>	99
---	----

L'evoluzione delle misure di sicurezza quale fattore di protezione dei dati. Un caso concreto <i>Pierangelo Felici</i>	105
--	-----

Interruzione volontaria di gravidanza e protezione dati personali: l'esempio spagnolo come modello per nuove linee guida del Garante della Privacy? <i>Maria Angela Pisanu</i>	110
--	-----

I sistemi di videosorveglianza in azienda: un delicato bilanciamento fra i tanti diritti in gioco <i>Eleonora Mataloni</i>	119
--	-----

Sezione III - Digitalizzazione, privacy e processo

L'evoluzione del processo tributario sospeso tra carta e digitale <i>Antonella D'Iorio</i>	130
---	-----

La riforma Cartabia e la specifica applicazione del diritto all'oblio agli imputati o ai soggetti indagati <i>Simonetta Zingarelli</i>	139
--	-----

EDITORIALE

Questo numero, dedicato a “*I professionisti della custodia di contenuti digitali*” è stato curato da Andrea Lisi, avvocato, esperto di diritto dell’informatica e di informatica giuridica. Il volume è strutturato in tre parti: dopo una sezione introduttiva, la prima parte è dedicata alla evoluzione digitale degli archivi; la seconda parte tratta della custodia dei dati; la terza parte si occupa della digitalizzazione, privacy e processo. Le parole chiave di questa monografia sono: custodia, contenuti digitali, professionisti. I *contenuti digitali* oggi sono trattati con le tecnologie dell’informazione e della comunicazione e quindi con una potenzialità di trattamento molto forte e sono quindi accessibili da parte di tutti coloro che operano in rete. I contenuti possono essere trattati/manipolati nel senso che in rete possiamo trovare contenuti di difficile/certa attribuzione per quanto attiene gli autori e la fonte dei documenti; contenuti che devono essere trattati secondo formati che interessano la formazione, la gestione, la conservazione dei documenti. Contenuti che interessano tutte le attività della società contemporanea: dalle attività sociali a quelle economiche, da quelle culturali e scientifiche a quelle tecniche, da quelle istituzionali a quelle amministrative, i settori pubblici e privati. La produzione di dati oggi è elevatissima proprio in relazione all’utilizzo delle tecnologie dell’informazione e della comunicazione. Contenuti di diversi livelli qualitativi che sono erogati, fruiti, conservati, diffusi in modalità digitale. Questi contenuti devono essere custoditi sia per conservarne la memoria (la esistenza dei contenuti) sia per collocare gli stessi contenuti nella loro storia e filiera di formazione, gestione, conservazione. La *custodia* di questi dati digitali richiede una specifica professionalità (per la formazione, la gestione, la conservazione dei dati). In questo numero dedicato appunto ai *professionisti della custodia dei dati digitali* sono stati affrontati diversi aspetti di questa professione: antica, perché la conservazione dei dati/documenti è ormai datata da migliaia di anni; nuova, rispetto all’utilizzo di tecnologie e alla tipologia dei dati/documenti formati, gestiti, conservati in modalità digitali e nel rispetto della loro integrità, del loro valore informativo e documentale, dei soggetti che hanno prodotti questi dati/documenti.

Il volume è presentato dal curatore, Andrea Lisi, che si occupa della costruzione delle competenze interdisciplinari come presupposto indispensabile per la crescita digitale del Paese. Tutto il volume è dedicato alle “competenze interdisciplinari”: un contributo utile per coloro che si dedicano e che si dedicheranno, sempre più numerosi, alla formazione, alla gestione, alla conservazione dei dati/documenti digitali.

Il Direttore della Rivista
Donato A. Limone

PRESENTAZIONE

Andrea Lisi

La costruzione di competenze interdisciplinari come presupposto indispensabile per la crescita digitale del Paese

Abstract: Il processo di digitalizzazione del Paese, nonostante gli obiettivi ambiziosi perseguiti dal Codice dell'Amministrazione digitale, sembra incontrare delle sostanziali difficoltà nella sua effettiva realizzazione. La questione tocca più da vicino le Pubbliche Amministrazioni, ancorate a sistemi obsoleti e contorti che vedono sempre più lontano il fine ultimo di una trasformazione digitale completa ed effettiva. Ad oggi non si tratta solo di un problema di natura tecnologica ma soprattutto di organizzazione e di sviluppo di competenze interdisciplinari, misure adatte a semplificare delle procedure ancora complesse e a disegnare un futuro affidabile ai dati, alle informazioni e ai documenti informatici del nostro Paese.

Nel presente lavoro verranno affrontate tematiche legate al processo di digitalizzazione in atto e alla custodia dei dati e dei contenuti digitali, analizzate sotto diversi profili che ci toccano da vicino per la loro attualità.

Despite the ambitious objectives pursued by the Digital Administration Code, the country's digitization process seems to be difficult in its effective implementation. The issue affects Public Administrations more closely, anchored in obsolete and convoluted systems that see the ultimate goal of a complete and effective digital transformation increasingly distant. Currently it is not just a technological problem but, above all, an organization and development of interdisciplinary skills matter, measures suitable for simplifying still complex procedures and designing a reliable future for data, information and IT documents in our country.

In this work, issues related to the digitization process in progress and the custody of data and digital content will be addressed and analysed under different profiles that touch us closely due to their relevance.

Parole chiave: digitalizzazione – competenze – codice dell'amministrazione digitale – pubblica amministrazione – dato – documento informatico – conservazione documentale

Sommario: 1. Premesse – 2. La digitalizzazione nelle PA: un processo non solo tecnologico – 3. Rifondare il Paese grazie alle competenze specialistiche – 4. L'importanza dei DPO per proteggere e custodire il nostro patrimonio informativo

1. Premesse

L'art. 12 del Codice dell'amministrazione digitale (in seguito CAD) chiede a tutte le pubbliche amministrazioni di organizzare autonomamente la propria attività utilizzando le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese. La centralità dei diritti di cittadini e imprese consente di interpretare correttamente anche lo spirito del successivo articolo 15, il quale precisa che gli obiettivi delineati dall'art. 12 devono essere perseguiti attraverso una **riorganizzazione strutturale e gestionale** delle pubbliche amministrazioni che avviene **anche** attraverso il migliore e più esteso utilizzo delle **tecnologie dell'informazione e della comunicazione** nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.

2. La digitalizzazione nelle PA: un processo non solo tecnologico

Quindi, correttamente, secondo il legislatore italiano **la digitalizzazione negli enti pubblici non è questione solo tecnologica, ma appunto organizzativa** (come del resto deve essere anche per gli enti privati) in modo da mettere al centro il cittadino nello sviluppo dei servizi on line. Per raggiungere questo fine ultimo della normativa occorre, quindi, **partire dalla definizione di ruoli e responsabilità**, finalizzando procedure, processi e procedimenti che possano portare con cognizione di causa verso un *agere* amministrativo meno burocratico, perché reso più semplificato e trasparente attraverso un utilizzo sapiente del digitale. E l'uso consapevole del digitale comporta necessariamente una **costruzione coerente di competenze interdisciplinari** dedicate a rinnovare i modelli organizzativi attraverso l'onda lunga della digitalizzazione.

Ma siamo purtroppo ancora molto lontani dal reale perseguimento di questi obiettivi. Del resto, ci sono **tre articoli** del CAD ancora oggi quasi totalmente **inapplicati**:

- **l'art. 8** che prevede di favorire, anche attraverso il servizio radiotelevisivo, la cultura digitale per tutti i cittadini (in particolare i minori) attraverso lo sviluppo di competenze di informatica giuridica e incentivando l'utilizzo dei servizi digitali. Purtroppo, non ci sono programmi dedicati a queste tematiche nel servizio radiotelevisivo nazionale.
- **l'art. 13** che chiede a tutte le pubbliche amministrazioni nell'ambito delle risorse finanziarie disponibili di attuare politiche di reclutamento e

formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione e, in particolare, volte allo sviluppo delle competenze tecnologiche, di informatica giuridica e manageriali. Difficile trovare traccia di concorsi pubblici focalizzati su queste competenze interdisciplinari.

- **l'art. 17** chiede alle pubbliche amministrazioni di garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo e, a tal fine, impone a ciascuna pubblica amministrazione di affidare a un unico ufficio dirigenziale generale la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Il responsabile di questo ufficio di transizione al digitale deve essere dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali. Ad oggi, non è purtroppo consueto incontrare, quando sono stati formalmente designati, manager della transizione digitale con tali profili interdisciplinari.

Il rischio di tale situazione è che si continui a sviluppare **una digitalizzazione troppo spesso improvvisata**, poco sistematica, contorta e inutilmente burocratica, proprio perché non si è partiti con il piede giusto, come richiesto dal CAD e, cioè, da un profondo rinnovo delle competenze digitali del Paese.

Eppure, **dal 1° febbraio 2022 il Sistema Paese si è dotato del "Syllabus"**¹, il programma di assesment e formazione digitale voluto dal Dipartimento della Funzione Pubblica e rivolto ai dipendenti pubblici, nell'ambito del Piano strategico per la valorizzazione e lo sviluppo del capitale umano "Ri-formare la PA. Persone qualificate per qualificare il Paese". Ma i risultati ad oggi raggiunti con questo ambizioso progetto sono ancora frammentati e parziali nonostante fosse tutto gratuitamente a disposizione per gli enti pubblici che hanno deciso di partecipare. Del resto, 2561 pubbliche amministrazioni abilitate e 87.639 dipendenti pubblici che hanno completato il test non possono che farci comprendere che ancora siamo lontani da risultati davvero apprezzabili e rassicuranti per il nostro Paese. E non posso non chiedermi oggi se qualcuno si stia davvero preoccupando di controllare con attenzione se **i copiosi piani di finanziamento voluti dal PNRR**, che dovrebbero inondare di tecnologia digitale le PA Italiane, realmente perseguano questa fondamentale impostazione metodologica.

¹ Il Syllabus "Competenze digitali per la PA" è il documento che descrive l'insieme minimo delle conoscenze e abilità che ogni dipendente pubblico, non specialista IT, dovrebbe possedere per partecipare attivamente alla trasformazione digitale della pubblica amministrazione. Sulla piattaforma Syllabus i dipendenti individuati dalle amministrazioni possono accedere all'autovalutazione delle proprie competenze digitali. Informazioni complete sul progetto possono ricavarsi a questo link: <https://www.funzionepubblica.gov.it/formazione/syllabus-competenze-digitali>

3. Rifondare il Paese grazie alle competenze specialistiche

Il futuro digitale dell'Italia dipende dalla costruzione delle competenze atte a presidiare i processi di digitalizzazione perché non possiamo non sottolineare come siamo di fronte a un Paese che troppe volte ha assegnato confusamente poteri di natura pubblicistica a privati, senza rendersi conto che **per incidere sul diritto amministrativo ci vuole un bisturi, seppur digitale e non un martello pneumatico in mano a “manager del digitale”, magari mutuati dalla Silicon Valley**, i quali sono animati senz'altro dalle migliori intenzioni, ma non possono conoscere i dettagli del mondo complesso delle nostre PA. E allo stesso tempo non possiamo ancora oggi, nel 2023, a più di trent'anni dalle prime normative italiane sull'informatizzazione della PA, commettere il **grave peccato di burocratizzare il digitale**. Si chiede a increduli cittadini in tante pubbliche amministrazioni ancora oggi, troppo spesso e allegramente, di acquisire un modulo on line, stamparlo, firmarlo, scansionarlo e inviarlo via PEC (seguito dalla copia “fotostatica” del documento d'identità). Procedura giuridicamente ancora ammissibile, ma folle². E, se gli allegati pesano troppo, occorre anche recarsi allo sportello. E allo stesso tempo costituiscono un indigesto fritto misto le procedure di votazione ibride in uso in molti “innovativi” contesti: mezze analogiche e mezze digitali. Costosissime, cervelotiche e ambigue.

La digitalizzazione dovrebbe invece essere inclusiva, agevole e dovrebbe essere concepita solo per semplificare con arguta intelligenza e conoscenza dei principi generali da osservare. I principi sono quelli del diritto, ma anche dell'archivistica e vanno ridisegnati sapientemente e con coraggio nel loro incontro con la tecnologia. E infatti oggi dovremmo ripartire proprio dai principi generali, semplificando la copiosa e ingarbugliata normativa su cui si è posata l'innovazione digitale all'italiana, in modo da ricostruire i pilastri della digitalizzazione di questo Paese. Ma è questione che non può essere affrontata nelle poche righe di questo editoriale. Di certo però semplificare, sistematizzare e ripartire è possibile solo attraverso un approccio interdisciplinare e consapevole. Pertanto, **si deve necessariamente (ri-)partire dalle competenze, quindi, e non dalla tecnologia.**

Tra queste competenze ci sono due figure fondamentali che condividono l'acronimo, i DPO. I **Digital Preservation Officer** (o Responsabili della gestione e conservazione dei documenti informatici, come sono più conosciuti), i quali accanto ai **Data Protection Officer** (Responsabili della protezione dei dati personali) possono di-

² E non sorprende quindi la sentenza n. 5744, pronunciata il 19 gennaio 2023 dalla Terza Sezione Penale della Corte di Cassazione che ha dichiarato l'ammissibilità di un atto di appello stampato, scannerizzato e firmato digitalmente dal difensore. Si consiglia il commento alla sentenza di Carola Caputo su Filodiritto “Documento informatico e copia per immagine di documento cartaceo: la sottile (in)differenza secondo la Corte di Cassazione”: <https://www.filodiritto.com/documento-informatico-e-copia-immagine-di-documento-cartaceo-la-sottile-indifferenza-secondo-la-corte-di-cassazione>

segnare un futuro affidabile ai dati, informazioni e documenti informatici di questo Paese. Sono entrambe, infatti, figure strategiche e indispensabili per garantire quella compliance che le normative di settore pretendono nell'attuazione delle politiche di digitalizzazione documentale. Figure che vanno preparate al cambiamento di modelli e processi, dovendo esprimere anche doti manageriali per esercitare i compiti molto delicati che la normativa a loro attribuisce

4. L'importanza dei DPO per proteggere e custodire il nostro patrimonio informativo

Ovvio che tra Responsabili della protezione dei dati personali e Responsabili della gestione e conservazione di documenti informatici ci siano parallelismi e anche importanti differenze. Ma non possiamo non osservare come qualsiasi trattamento di dati personali debba garantire, secondo l'art. 5 del GDPR, i principi fondamentali di esattezza, integrità, riservatezza e limitazione della conservazione, oltre ovviamente a correttezza e trasparenza. Tali principi sono anche di derivazione archivistica e devono essere alla base di qualsiasi sistema di formazione, gestione e conservazione di documenti informatici. E, infatti, i principi di integrità, sicurezza, immutabilità, autenticità animano sia la normativa sulla trasparenza amministrativa (prevista nel D. Lgs. 33/2013) e sia la normativa sulla digitalizzazione documentale (contenuta nel CAD). **Non c'è, quindi, trasparenza senza un'efficace e corretta digitalizzazione, ma allo stesso tempo non c'è digitalizzazione senza protezione dei dati.**

Del resto, siamo ormai "datificati" e, proprio per questo, quei **dati che hanno un rilievo giuridico vanno garantiti** nella loro integrità e leggibilità, vanno correlati tra loro e resi accessibili nel tempo, quindi vanno documentati, fascicolati e archiviati. E, e non lo si garantisce, il valore giuridico di tutte quelle informazioni giuridicamente rilevanti ...evapora! *Bit volant*³, in poche parole.

Per tale motivo i DPO (intesi sia come digital preservation officer e sia come data protection officer) sono figure strategiche e, secondo il CAD e le Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, devono tra loro parlarsi e devono essere abituate ad agire in team a presidio di database e sistemi di gestione documentale. In particolare, il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia. La stessa autonomia e indipendenza da assicurare al DPO, il quale deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali in modo da considerare debitamente i rischi inerenti a tutti i trattamenti dei dati personali

³ E questo è infatti il titolo del mio blog ospitato da Filodiritto e disponibile in questa pagina web <https://www.filodiritto.com/rubriche/bit-volant>

posti in essere da enti pubblici e privati, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità.

Entrambe queste figure hanno ampi poteri di delega e possono svolgere anche altri compiti, purché compatibili con le specificità del loro ruolo. Addirittura, il CAD attribuisce al responsabile della conservazione il potere di affidare la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrano idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Mentre al DPO vengono attribuiti ampi poteri di ispezione e controllo, oltre che di esprimere pareri nei vari ambiti più delicati di trattamento dei dati personali.

Peraltro, entrambe queste figure possono essere esternalizzate, purché ovviamente il soggetto esterno all'organizzazione abbia quelle idonee competenze interdisciplinari che tali ruoli richiedono e garantisca terzietà nell'esercizio del delicato incarico⁴. Quindi, sono indispensabili per queste figure professionali autonomia e indipendenza, da una parte, ma anche capacità di organizzazione e di cooperazione, dall'altra. Perché il rischio è di rimanere altrimenti isolati. E non è compito semplice e ovvio questo, perché come affermava Pier Paolo Pasolini "l'indipendenza, che è la mia forza, implica la solitudine, che è la debolezza".

E la solitudine dei DPO si respira tristemente in tante, troppe PA.

⁴ Credo che sia doveroso precisare che le Linee Guida prevedono l'affidamento all'esterno di questo ruolo solo per i soggetti privati e non per quelli pubblici.

Autori di questo numero

Gabriele Bezzi

Archivista Funzionario della Regione Emilia-Romagna –Polo Archivistico Regionale (ParER) - Responsabile della funzione archivistica di conservazione. Laureato all'Università di Bologna in Storia contemporanea nel 1980 e diplomato in Archivistica, Paleografia e Diplomatica nel 1983 presso la scuola dell'Archivio di Stato di Bologna è dal novembre 2009 responsabile della funzione archivistica di conservazione del Polo Archivistico regionale dell'Emilia-Romagna: (ParER). In precedenza, è stato responsabile del servizio archivio e protocollo generale della Provincia di Bologna dal giugno 2000 all'ottobre 2009. Fin dalla metà degli anni '80 si è occupato dei rapporti tra archivistica e informatica contribuendo allo sviluppo di sistemi informatici di descrizione archivistica utilizzati nel corso di numerosi interventi di riordino ed inventariazione di fondi archivistici di diversi enti per poi, negli ultimi anni, approfondire i temi della gestione corrente e della produzione e conservazione di documenti informatici. Fin dai primi anni 2000, ha partecipato alle diverse edizioni del progetto internazionale sulla conservazione di risorse digitali Interpares e attualmente partecipa all'ultima Interpares Trust AI sull'applicazione dell'intelligenza artificiale nell'ambito degli archivi e della conservazione digitale.

Dimitri Brunetti

Professore associato di archivistica e archivistica digitale e coordinatore del Corso di studi in Beni Culturali presso l'Università degli Studi di Udine. Componente del Direttivo dell'Associazione italiana docenti universitari scienze archivistiche, membro del Comitato scientifico delle riviste «Archivi», «DigItalia», «Atlanti+» e «Journal of interactive books» e del Consiglio didattico del Corso di alta formazione in Archivistica contemporanea presso l'Archivio Centrale dello Stato. Per molti anni funzionario pubblico con responsabilità sui sistemi informativi archivistici, da tempo si occupa di gestione documentale e di transizione digitale, pubblicando nel 2005 per Maggioli il primo manuale sul Codice dell'amministrazione digitale. Si occupa anche della descrizione e valorizzazione dei fondi archivistici a valenza culturale, con particolare attenzione agli archivi degli enti locali e della creatività. Autore di numerose pubblicazioni, fa formazione per le pubbliche amministrazioni in materia di gestione dei documenti informatici.

Antonella D'Iorio

Avvocato, esperta in Protezione dei dati personali. Laureata in Giurisprudenza alla Federico II di Napoli, avvocato del foro di Torre Annunziata e titolare dello Studio Legale D'Iorio, fornisce assistenza nelle materie di diritto civile con particolare ap-

profondimento per le tematiche patrimoniali e familiari. Appassionata sulle questioni di abusivismo edilizio, diritto pubblico e procedure concorsuali, collabora con lo studio fondato dall'Avv. Prof. Giuseppe Abbamonte e Avv. Sergio Como in Napoli. Presso la Federico II di Napoli ha conseguito il diploma della scuola di specializzazione per le professioni legali (SSPL) e il master universitario di II livello in Arbitrato e Conciliazione. È mediatore civile e commerciale e mediatore familiare. Consulente in materia di “protezione dei dati” per imprese e privati svolta in qualità di libero professionista già per gli adempimenti al Codice della Privacy (d.lgs. 196/2003). Socio effettivo di Anorc iscritta dall'anno 2010 ad oggi. Ha conseguito il master di alta specializzazione in “Data Protection Officer” promosso da Euroconference (Centro studi forense) con il patrocinio di Anorc Professioni presso la sede di Roma. Attualmente iscritta al Mastercourse Executive per la formazione dei Responsabili della Conservazione e Conservatori di oggetti digitali promosso dall'Associazione ANORC e patrocinato da AgID.

Monica Del Rio

Funzionario archivista di Stato. Laureata in Lettere classiche presso l'Università degli studi di Padova, diplomata presso la Scuola di Archivistica Paleografia e diplomatica dell'Archivio di Stato di Venezia, si è specializzata in Innovazione, progettazione e valutazione delle politiche dei servizi (Master di II livello - Università degli di Padova, 2022). Dopo 10 anni di libera professione, dal 2012 è in ruolo come archivista di Stato presso l'Archivio di Stato di Venezia – Ministero della cultura, dove è responsabile del sistema informativo e delle attività di valorizzazione. Ha svolto attività didattica dal 2002, curando seminari di Archivistica per corsi dell'Università degli studi di Venezia, dello IUAV, dell'Università degli studi di Verona e dell'ANAI – Associazione nazionale archivistica italiana; attualmente è titolare dell'insegnamento di Archivistica e Sistemi di gestione documentale presso la Scuola di Archivistica, paleografia e diplomatica dell'Archivio di Stato di Venezia e docente per Università ed enti di formazione specialistica per pubblica amministrazione e professionisti.

Pierangelo Felici

Consulente di direzione, DPO. Professionista con oltre 20 anni di esperienza in Consulenza di Direzione sia per Enti Pubblici sia per Aziende private, anche di dimensione multinazionale, si occupa di coordinamento di progetti di innovazione, Data Protection e Privacy, ICT e organizzazione, sicurezza informatica, nuove tecnologie, temporary management, e della conseguente formazione del personale. Svolge in particolare consulenza, audit e attività di formazione negli ambiti della Protezione dei Dati, Privacy e compliance GDPR, Trasformazione Digitale, Cybersecurity, E-Government e Innovazione della Pubblica Amministrazione, conservazione e gestione documentale digitale. Si è occupato di innovazione e interscambio su dati ad alta rilevanza anche in progetti pilota a livello locale e nazionale, di sviluppo di Modelli di Organizzazione e Gestione ex D.Lgs. 231/2001 per la riduzione del rischio-reato nelle imprese, e di adempimenti connessi alle normative antiriciclaggio ed alle pro-

cedure tributarie e di compliance normativa. Ricopre la funzione di Data Protection Officer (DPO – RPD) ex Regolamento (UE) 679/2016 - GDPR per diversi Enti Pubblici locali e per imprese nei settori manifatturiero, ICT, socio assistenziale e sanitario.

Luigi Foglia

Avvocato (Foro di Lecce dal 2009), consulente esperto in diritto dell'informatica e archivi digitali. Collabora con lo Studio Legale Lisi dal 2009, occupandosi principalmente di diritto dell'innovazione digitale, contratti di outsourcing informatico, formazione e conservazione digitale del documento informatico, firme elettroniche, fatturazione elettronica, innovazione nella PA, privacy, licenze d'uso software e disaster recovery. Segretario generale di ANORC, riveste inoltre il ruolo di Responsabile della conservazione per conto della stessa Associazione. È inoltre iscritto nell'Elenco della sezione "Professionisti della digitalizzazione" – Livello EXPERT, tenuto da ANORC Professioni.

Patrizia Gentili

Consulente e docente in materia di digitalizzazione. Già Responsabile Servizio Documentali e Servizio documentale e modelli di marcatura presso AgID, Patrizia Gentili è un'esperta di Digitalizzazione e svolge attività freelance di consulenza e docenza in materia.

Andrea Lisi

Avvocato. Si occupa di diritto applicato all'informatica da più di 20 anni. Oltre allo Studio Legale Lisi, coordina le realtà di Digital&Law e D&L NET ed è l'ideatore della piattaforma DIGEAT +. Dal 2023 è Componente nel Comitato di Esperti di comprovata esperienza e qualificazione in materia di innovazione tecnologica e transizione digitale della PA che affiancherà il Sottosegretario alla Presidenza del Consiglio con delega all'Innovazione tecnologica, Sen. Alessio Butti per guidare la trasformazione digitale del Paese. È il Presidente di ANORC Professioni e Presidente Onorario di ANORC. Collabora in tutta Italia con enti pubblici e aziende private, enti camerali, centri di ricerca, primarie società fornendo progettazione, formazione, assistenza e consulenza legale sugli aspetti giuridici della digitalizzazione, della contrattualistica informatica, dell'e-commerce e dell'e-gov, della sicurezza informatica e della protezione dei dati. Riveste il ruolo di Direttore scientifico di numerosi Master e percorsi specialistici di settore, organizzati in collaborazione con Università ed Enti di Formazione nazionali. È blogger su argomenti inerenti al diritto applicato all'informatica per Huffington Post, Il Fatto Quotidiano, Key4biz.it e Filodiritto curatore della trasmissione "Lo ho-BIT – una digicrazia inaspettata" ospitata su MRTV.it.

Eleonora Mataloni

Avvocato. Laurea in Giurisprudenza nel 2007 con lode e riconoscimento della Dignità di Stampa della Tesi di Laurea in Diritto dell'Unione Europea; 2010: abilita-

zione alla Professione Forense. Avvocato civilista con consolidata esperienza in materia ereditaria e successoria nonché immobiliare e nel diritto del web; consulente privacy – GDPR, esperta di e-commerce, compliance aziendale, digital marketing, proprietà intellettuale, marchi e brevetti. Da luglio 2018: iscrizione all’Elenco dei Professionisti della privacy di ANORC Professioni – Professionisti della Privacy – Tessera n. 42; Da giugno 2022: iscritta nell’Albo Maestri IIP – presso l’Istituto Italiano Privacy. Svolge il ruolo di DPO – Responsabile per la protezione dei dati personali, sia in ambito privato sia a favore di Enti pubblici.

Enrico Pelino

Avvocato, esperto in diritto digitale e della protezione dei dati personali, sicurezza informatica, DPO. Civilista di formazione, è appassionato delle frontiere del diritto. Si occupa inoltre di diritto del lavoro e contrattualistica. Svolge attività di assistenza in contenzioso e attività consulenziale e stragiudiziale. In particolare, in ambito di protezione dei dati personali assiste i proprio clienti in: procedure avanti al Garante per la protezione dei dati personali e connessi procedimenti giudiziari, gestione di data breach, analisi dei rischi (LIA, TIA, RIA, ecc.) e valutazione d’impatto (DPIA), gap analysis e percorsi di adeguamento e conformità, redazione e verifica di policy aziendali, tutela dei dati personali nei luoghi di lavoro, controlli su posta elettronica e Internet, gestione di diritti GDPR, profili penalistici quali accesso abusivo a sistemi informatici, furto d’identità. Si occupa altresì di protezione dell’identità online, cloud computing, tutela di dati personali in ambito sanitario. È PhD in IT Law (Università di Bologna), Privacy Expert di Anorc Professioni, Fellow dell’Istituto Italiano Privacy, avvocato della rete D&L Net di professionisti della protezione dei dati personali. Svolge e ha svolto attività di docenza e formazione di alto livello/master rivolti a professionisti e imprese, per Anorc, Unitelma, Istituto Italiano Privacy, Università Ca’ Foscari, Euroconference. Pubblica contributi in numerose riviste del settore, collabora a volumi di approfondimento giuridico (es. in materia di class action per Giuffrè, 2021), ed è co-autore e co-direttore di opere di commento giuridico quali “Codice della disciplina privacy” (Giuffrè 2019), “CODICE PRIVACY: tutte le novità del D.lgs. 101/2018” (Giuffrè 2018), “Il Regolamento privacy europeo” (Giuffrè 2016). È ospite radiofonico consueto di IusLaw Web Radio – La radio dell’avvocatura. È relatore in convegni ed eventi che riguardano il diritto digitale e la protezione dei dati personali.

Andrea Piccoli

Ingegnere, Professionista della digitalizzazione e privacy. Opera come professionista della digitalizzazione e privacy, offrendo attività di consulenza nel disegno, conduzione e valutazione dei sistemi di gestione in ambito sicurezza e protezione dei dati personali; in un modello multidisciplinare ed integrato, che contempla sia gli aspetti di organizzazione delle persone e dei processi, sia quelli legati alle tecnologie e alle valutazioni di conformità e audit. La proposta di valore è quindi quella di affiancarsi alle direzioni degli enti e aziende nell’approccio alla complian-

ce aziendale gestendo ed applicando la digitalizzazione dei procedimenti e attività, ottenendo maggiore efficacia ed efficienza degli stessi. Segue la normativa ed applicazione del riuso nella pubblica amministrazione con particolare riferimento alle soluzioni di gestione documentale, protocollo informatico e conservazione. Il suo ruolo consulenziale è orientato all'accompagnamento degli enti e delle aziende nella applicazione della digitalizzazione dei propri procedimenti e attività a norma con una gestione archivistica e conservazione digitale. La gestione documentale è anche lo strumento principe per condurre e raccogliere le evidenze relative alla governance della compliance di un ente o azienda, dal GDPR, alla qualità (ISO 9001), alla sicurezza (ISO 27001), e ai sistemi di gestione delle certificazioni verticali di settore; così come strumento di trasparenza dell'azione amministrativa verso i cittadini digitali. Assume, a vario titolo, il ruolo di responsabile della conservazione o suo delegato e di quello di funzione archivistica, sia in contesti di Pubbliche Amministrazioni che di aziende private, curando i rapporti con i conservatori accreditati o assumendo i ruoli previsti dalla norma all'interno dei conservatori stessi. Per le tematiche del GDPR è valutatore certificato per lo schema ISPD 10003:2020 accreditato per la valutazione di conformità al GDPR in forma volontaria: l'adozione di schemi di valutazione riconosciuti permette di avere una maggiore consapevolezza del Titolare per la sua accountability. Si interessa delle applicazioni della IA basate su indicizzazione semantica dei documenti e classificazione, iscritto all'elenco Innovation Manager del MISE. All'interno di ANORC e ANORC Professioni partecipa a diversi tavoli di lavoro sia sulle evoluzioni normative che riguardano la digitalizzazione e conservazione digitale, sia sulle nuove tecnologie come quella dei DTM, machine learning applicato ai procedimenti amministrativi e indicizzazione semantica. E' delegato territoriale di ANORC Triveneto e coordina gli iscritti del territorio ad ANORC Professioni e ANORC Mercato. Ha un incarico come esperto presso il Dipartimento della Trasformazione Digitale, Presidenza del Consiglio dei ministri, dove opero come Account Manager nel Nord-Est Accompagno le Pubbliche Amministrazioni del Veneto, Trentino Alto-Adige, Emilia-Romagna, Friuli-Venezia Giulia alla adesione e partecipazione ai bandi del PNRR previsti da Strategia PA 2026. Collabora per individuare le strategie per il coinvolgimento degli enti e del successo delle progettualità previste dalle misure.

Maria Angela Pisanu

Assistente Amministrativa Comparto Scuola (ATA). Laureata in Scienze Politiche all'Università degli Studi di Cagliari e specializzata in Comunicazione Pubblica e Project Management all'IED di Milano. Ha maturato esperienza professionale principalmente nella Sanità Pubblica (servizi di data entry, segretariato, sportello settore CUP e Ticket, gestione rapporti con gli utenti) e a seguire nel comparto Scuola come assistente amministrativa (Graduatorie ATA).

Nel 2020 ha conseguito la CERTIFICAZIONE LIVELLO EQF/QNQ: 6 (Percorso ECompetence: Framework per la Sardegna) nell'ambito della disciplina vigente in materia di protezione dati (GDPR 679/2016 e D. Lgs. 196/2003), sotto la guida del Prof.

Massimo Farina. Ha acquisito dimestichezza nella redazione generale di testi documentali e nella redazione di adempimenti privacy (quali informative, registri, pareri, notificazioni e comunicazioni), con un occhio attento soprattutto ai principi, ai diritti dell'interessato e all'etica della protezione dati. Da gennaio 2020, compatibilmente con l'impegno nel comparto scuola, svolge attività di consulenza e formazione per piccole realtà imprenditoriali sarde in ambito privacy & data protection. Parallelamente si occupa di scrittura, editing e ghostwriting, mantenendosi costantemente aggiornata attraverso i corsi multidisciplinari della community "Come si scrive una grande storia", scuola di scrittura e sceneggiatura fondata da Francesco Trento.

Micaela Procaccia

Presidente Associazione nazionale archivistica italiana. Fino al 30 aprile 2019 dirigente del Servizio Patrimonio archivistico della Direzione generale archivi, poi Presidente ANAI. Componente del CTS Archivi del Ministero della cultura, componente del CdA dell'Istituto centrale per la digitalizzazione del patrimonio culturale, componente di diversi gruppi di lavoro italiani e internazionali relativi al settore degli archivi, autrice di testi relativi al settore e di ricerca storica.

Alessandro Selam

Giurista - Responsabile della Direzione di ANORC. Si occupa dei rapporti istituzionali di ANORC Mercato e ANORC Professioni e ne rappresenta gli interessi nei rapporti con la Camera dei deputati sin dal 2018. Già componente del Consiglio Direttivo UNINFO, Ente Federato UNI per la normazione delle "Tecnologie Informatiche e loro applicazioni" (04/2016-04/2022) e Componente del Consiglio Direttivo del CoLAP, Coordinamento Libere Associazioni Professionali 06/2017-01/2023).

Sarah Ungaro

Avvocato del Foro di Lecce. Consulente esperta in diritto dell'informatica e protezione dei dati personali. Ha conseguito il diploma della Scuola di Specializzazione per le professioni legali. Collabora con lo Studio Legale Lisi in qualità di consulente senior in materia di diritto dell'informatica, protezione dei dati personali, e-government, contratti IT, cloud, blockchain, AI, proprietà intellettuale, e-health, fascicolo sanitario elettronico, telemedicina, documento informatico, trasparenza amministrativa, open data, riuso, firme elettroniche, dematerializzazione dei documenti contabili e fiscali, conservazione digitale, fatturazione elettronica, appalti e e-procurement. In relazione a tali materie, è docente per Università ed enti di formazione specialistica pubblici e privati, partecipa in qualità di relatrice a seminari e convegni ed è autrice di numerose pubblicazioni su testate specialistiche di settore. Vice Presidente dell'associazione ANORC Professioni, ne è componente della Commissione di valutazione ed è iscritta nell'Elenco della sezione "Professionisti della digitalizzazione" – Livello EXPERT e nell'Elenco della sezione "Professionisti della privacy" – Livello EXPERT, tenuti dalla stessa associazione. Iscritta all'Albo dei Maestri Protezione Dati & Data Protection Designer® IIP.

Giuseppe Vitrani

Avvocato del libero foro (Torino) con competenze in diritto commerciale e dell'informatica. Esperto di conservazione dei documenti informatici, materia nella quale ha conseguito anche il Master in formazione, Gestione e Conservazione di Archivi Digitali presso l'Università di Macerata.

Simonetta Zingarelli

Avvocato, Foro di Lecce; consulente esperta in diritto dell'informatica. Avvocato Civilista, specializzata in diritto dell'informatica e protezione dei dati personali. Si occupa di consulenza e formazione in materia di e-governement, conservazione digitale dei documenti e trattamento dei dati personali per imprese e PA. Consulente dello Studio Legale Lisi e tesoriere dell'Associazione ANORC.

LA CUSTODIA DEL PATRIMONIO INFORMATIVO PUBBLICO: UN'INDAGINE A CURA DI ANORC

Alessandro Selam

Abstract: ANORC Mercato e ANORC Professioni hanno avviato una rilevazione sull'adempimento dell'obbligo di pubblicazione della nomina del Responsabile della conservazione e della pubblicazione del Manuale di conservazione estesa a un campione rilevante costituito da 288 Enti pubblici. L'indagine ha avuto inizio nel giugno del 2022 e non caso in quello che verosimilmente può essere considerato il momento storico più adatto a evidenziare e risolvere le eventuali carenze nella gestione del patrimonio informativo e documentale prevalentemente per tre ragioni: la sedimentazione della normativa di riferimento, la predisposizione post pandemica dei cittadini all'utilizzo della tecnologia e la disponibilità di risorse utili alla realizzazione di progetti importanti che il PNRR può garantire.

In questo articolo si presentano i primi risultati conseguiti, certamente suscettibili di futuri aggiornamenti e rielaborazioni, ma che al momento costituiscono una fotografia emblematica dello stato di consapevolezza generale della Pubblica Amministrazione nazionale nei riguardi della corretta gestione e conservazione del patrimonio informativo che ci appartiene.

ANORC Mercato and ANORC Professioni have launched a survey on the fulfilment about the obligation to publish the appointment of the Record Manager and the publication of the Record Manual extended to a relevant sample made up of 288 public bodies. The survey began in June 2022 and not by chance in what can probably be considered the most suitable historical moment to highlight and resolve any deficiencies in the management of information and documentary assets mainly for three reasons: the sedimentation of the reference legislation, the post-pandemic predisposition of citizens to the use of technology, and the availability of resources useful for the realization of important projects that PNRR can guarantee.

This article presents the first results achieved, certainly susceptible to future updates and reworkings, but which now constitute an emblematic snapshot of the general state of awareness of the national Public Administration with regard to the correct management and conservation of the information assets that belong to us.

Parole chiave: indagine – pubblica amministrazione – trasparenza – conservazione – dati – informazioni – documenti – Responsabile della Conservazione – Manuale di Conservazione

Sommario: 1. Il contesto della rilevazione – 2. Le prime fasi della rilevazione – 3. Lo scopo della rilevazione - 4. Una fotografia della custodia del patrimonio informativo pubblico.

Apparteniamo ad una società che si nutre incessantemente di informazioni con ogni mezzo e modalità, per le più svariate finalità e proprio il trattamento di dati, informazioni e documenti è oggetto dell'attenzione del nostro Legislatore ormai da oltre un ventennio.

Per il ruolo preminente che possono rivestire nel rapporto con i soggetti di diritto, gli Enti pubblici sono assoggettati nel nostro Paese a una normativa specifica e decisamente articolata in materia. La **normativa sulla trasparenza** (Decreto Legislativo 14 marzo 2013, n. 33) ne è una componente essenziale ed è stata introdotta nel nostro ordinamento con il preciso scopo di **favorire forme diffuse di controllo sull'azione amministrativa**, sull'utilizzo delle risorse pubbliche e sulle modalità con le quali le PP.AA. agiscono per raggiungere i propri obiettivi.

Negli ultimi anni abbiamo assistito al moltiplicarsi delle notizie che raccontano di progetti di **PA Digitale, smart city, identità** e uno spazio sempre maggiore occupano anche i comunicati che presentano **piattaforme nazionali che propongono nuovi accessi e nuove opportunità tramite servizi "innovativi"**. In questi casi l'entusiasmo prende il sopravvento, facendo pensare a quanto sarebbe magnifico poter ritrovare nel rapporto con la PA la medesima usabilità che si riscontra nei rapporti tra privati e nello specifico nei rapporti con le più famose piattaforme social (ma non solo). Tuttavia, la realtà continua a differire enormemente dalle aspettative. Per questo ANORC Mercato e ANORC Professioni hanno deciso di intraprendere una **rilevazione su scala nazionale**, per tastare il polso degli Enti sul tema della formazione, gestione e conservazione dei documenti informatici e, in particolare, della programmazione e implementazione dei processi necessari per l'adempimento di una parte degli obiettivi previsti dal Legislatore.

1. Il contesto della rilevazione

Si è ritenuto che quello attuale fosse **il momento storico più adatto**¹ a evidenziare e risolvere le eventuali carenze nella gestione del patrimonio informativo e documentale prevalentemente per tre ragioni: la sedimentazione della normativa di riferimento, la predisposizione post pandemica dei cittadini all'utilizzo della tecnologia e la disponibilità di risorse utili alla realizzazione di progetti importanti che il PNRR può garantire.

¹ Questi di seguito riportati sono i dati a fine 2022 presentati nel Report annuale di ForumPA srl. Le identità digitali SPID sono arrivate a 33,5 milioni (erano 27,4 milioni a fine 2021), mentre le carte d'identità elettroniche (CIE) a 32,7 milioni (25,9 a fine 2021). E aumenta il numero di amministrazioni che consentono l'accesso ai servizi online: oltre 12.500 le PA attive su SPID (9.200 a fine 2021), oltre 6.200 quelle con l'autenticazione tramite CIE. È proseguita la crescita esponenziale di pagamenti digitali attraverso pagoPA, di cui nel 2022 sono state eseguite circa 332 milioni di transazioni, +103% rispetto al 2021, per oltre 61 miliardi di euro (+80% rispetto all'anno precedente). L'app IO ha oltre 32,3 milioni di download (erano 24,5 milioni a fine 2021), con più di 12.200 PA attive (contro le circa 6.900 del 2021) e 171.000 servizi disponibili (contro i 77.000 dell'anno precedente).

In Italia non si può parlare più di “novità”, poiché la normativa di settore risale alla fine degli anni '90. Certamente, di recente sono stati apportati dei miglioramenti sia in ambito europeo, che nazionale, ma senza particolari stravolgimenti. **Il primo gennaio 2022 è stato il giorno “0” per la piena attuazione delle LLGG AgID sulla formazione, gestione e conservazione dei documenti informatici.** Una partenza che ha potuto contare su un lungo periodo di preparazione e di adattamenti.

Pubblicate nel corso del 2020, infatti, le LLGG hanno previsto un lungo periodo di adeguamento, che poteva e doveva essere ben sfruttato per recuperare quanto non sviluppato negli anni precedenti. Si deve ricordare che **le LLGG non rappresentano nulla di nuovo.** La formazione, gestione e conservazione dei documenti informatici dovevano già essere una realtà – perché questo prevedeva la normativa primaria – da molti anni.

Con la necessità di gestire il quotidiano in modalità remota, sperimentata a causa della pandemia di Covid 19, l'utilizzo dei servizi digitali si è largamente esteso anche alla fetta di popolazione che resisteva al processo di digitalizzazione, generando tra l'altro una corrente di critica costruttiva che si è riverberata nei confronti del processo di digitalizzazione, con effetti decisamente positivi in termini di progresso sull'usabilità, sulla fiducia e, in alcuni casi, anche sulla comprensione dei processi sottostanti.

Certamente quanto di positivo è germogliato dalle ceneri della pandemia non può essere considerarlo sufficiente per la piena realizzazione della trasformazione digitale del nostro Paese. I progetti da implementare sono ancora numerosi e, considerato l'elevato numero di pubbliche amministrazioni locali e la natura del territorio che le ospita, le risorse economiche da impegnare per questi progetti non è certo indifferente. In questo contesto occorre prestare attenzione alle **opportunità che possono derivare dai fondi del PNRR.** Si tratta di risorse strategiche per consentire al nostro Paese di raggiungere il posto che merita nelle classifiche internazionali della digitalizzazione e della crescita infrastrutturale.

2. Le prime fasi della rilevazione

Con spirito assolutamente collaborativo e con l'intento di sfruttare un momento storico particolarmente propizio, ANORC Mercato e ANORC Professioni hanno iniziato una rilevazione sui dati relativi **all'adempimento dell'obbligo di pubblicazione della nomina del Responsabile della conservazione e della pubblicazione del Manuale di conservazione** sul sito istituzionale.

L'indagine ha ricompreso alcune categorie di Pubbliche amministrazioni, che per ragioni di storia, dimensioni e/o importanza istituzionale o territoriale, possono rappresentare il punto di partenza per una riflessione che possa estendersi ad una mappatura completa dello stato della digitalizzazione della nostra PA. **Il campione è costituito da 288 Enti**, nello specifico: gli Organi costituzionali e di rilievo costi-

tuzionale, la Presidenza del Consiglio dei Ministri e i Ministeri, le Agenzie fiscali, gli Enti di regolazione dell'attività economica, gli Enti produttori di servizi economici, le Autorità amministrative indipendenti, gli Enti a struttura associativa, gli Enti produttori di servizi assistenziali, ricreativi e culturali, gli Enti e Istituzioni di ricerca, gli Istituti zooprofilattici sperimentali, le Regioni, le Province Autonome, le Città Metropolitane e le Aziende sanitarie, gli stessi Enti che sono stati indicate dall'ISTAT nella serie generale della Gazzetta Ufficiale n. 234 del 30 settembre 2021 (Elenco delle amministrazioni pubbliche inserite nel conto economico consolidato individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, e successive modificazioni - Legge di contabilità e di finanza pubblica).

La prima fase dell'indagine si è concentrata sulla rilevazione del dato nomina del Responsabile della conservazione e della pubblicazione del Manuale della conservazione, **accedendo direttamente al sito istituzionale del singolo ente e verificando la pubblicazione degli atti** e documenti oggetto della rilevazione anche attraverso la funzione "ricerca" nella sezione trasparenza. **Questa prima fase si è svolta tra giugno e settembre 2022.**

La seconda fase della rilevazione è stata caratterizzata dalla condivisione delle informazioni raccolte con l'Ente interessato al fine di confermarne l'esattezza. Questa seconda fase si è protratta **fino al mese di gennaio 2023**, attendendo (molto spesso invano) il riscontro da parte delle PP.AA.

3. Lo scopo della rilevazione

È doveroso chiarire che lo scopo di questa indagine non è certo quello di giungere ad una valutazione in termini di "buoni o cattivi" in base al mero adempimento di un obbligo normativo. Il fine ultimo delle Associazioni promotrici, partendo dalla rilevazione del dato "puro", è quello di **stimolare il ragionamento e poter comprendere verosimilmente quanti Enti abbiano implementato un approccio virtuoso al tema della trasformazione digitale**, entrando nel merito della questione documentale, ponendosi dei quesiti e cercando di comprendere quale fosse la reale esigenza da soddisfare.

La necessità di rendere disponibile ai cittadini il Manuale della conservazione e la possibilità di reperire l'atto di nomina del Responsabile della conservazione si riferisce, ovviamente, alla necessità di trasparenza nell'operato della PA, ma non si tratta certamente solo di questo. La pubblicazione stessa rappresenta l'ultimo anello di un percorso di analisi e valutazione interna, propedeutica all'eventuale semplificazione e reingegnerizzazione dei processi e delle procedure dell'Ente.

Appare indubitabile che la valutazione dei processi in un'ottica di semplificazione e di adattamento ai nuovi strumenti di lavoro sia il presupposto imprescindibile per la corretta transizione digitale e soprattutto per gli effetti di efficacia, efficienza e economicità che la stessa potrebbe garantire.

4. Una fotografia della custodia del patrimonio informativo pubblico

Purtroppo la rilevazione ha espresso dati inaspettatamente bassi in riferimento agli adempimenti previsti.

Solamente il **4,9** % degli Enti visitati era perfettamente in regola con la doppia pubblicazione del Manuale di conservazione e dell'atto di nomina del Responsabile della conservazione.

Al termine del mese di settembre 2022 solamente l'**11,4** % degli enti visionati risultava aver pubblicato solo il Manuale della conservazione aggiornato alle LLGG AgID del 2020. Il dato percentuale migliora di poco (12,15 %) se si allarga la rilevazione ai Manuali di gestione (aggiornati) e sale fino al 19,4 % se si considerano anche i manuali di gestione non aggiornati e prodotti a partire dal 2006.

Altrettanto sconfortanti, se non peggio, risultano i dati sulla pubblicazione dell'atto di nomina del Responsabile della conservazione. A settembre 2022 la nomina era stata pubblicata solo dal **10,4** % delle 288 PP.AA. sottoposte a rilevazione. La percentuale degli Enti in regola con la pubblicazione dell'atto di nomina sale al 13,8 % se si tengono in considerazione anche gli atti di nomina pubblicati in seguito alla PEC di ANORC, quelli comunicati dall'Ente ad ANORC ma non pubblicati, i nominativi presenti nel Manuale ma senza atto di nomina formale e gli atti di nomina che riportano un nominativo differente da quello indicato nel Manuale.

Volendo fare qualche esempio concreto sulla situazione rilevata si riportano qui di seguito alcuni dati per tipologia di Ente, seguendo la classificazione proposta dall'ISTAT:

- nell'ambito delle Aziende sanitarie **2 su 98 Enti** (- 2,04 %) sono risultate in regola su entrambi gli adempimenti;
- nell'ambito della Presidenza del Consiglio dei Ministri e di tutti i Ministeri solamente **1 su 16 Enti** (- 6,25 %) è risultato in regola su entrambi gli adempimenti;
- nell'ambito delle Autorità Amministrative Indipendenti **1 su 9 Enti** (- 11, 11 %) è risultata in regola su entrambi gli adempimenti;
- nell'ambito degli Enti e Istituti di ricerca **3 su 26 Enti** (- 11, 53 %) sono risultati in regola su entrambi gli adempimenti;
- nell'ambito delle Agenzie fiscali nessuna (su 3 Enti totali) è risultata in regola su entrambi gli adempimenti;

Prendendo in esame i dati che provengono dagli Enti territoriali maggiori la situazione è invariata.

- nell'ambito delle Regioni **4 su 20 Enti** (- 20%) sono risultate in regola su entrambi gli adempimenti;
- nell'ambito delle Città Metropolitane **NESSUNA** (su 14 Enti totali) è risultata in regola su entrambi gli adempimenti.

La lettura dei dati raccolti ci suggerisce che con tutta probabilità **non è stata compresa l'importanza del ciclo di vita del dato e del documento informatico**, che rappresentano già oggi e sempre più in futuro la base per la memoria del nostro Paese. Occasioni come questa sono il momento per riflettere attentamente sull'opportunità di perseguire la strada delle riforme "a costo zero" e di decidere di investire seriamente sulle competenze davvero utili.

Sarebbe meraviglioso se anche nel nostro Paese si riuscisse a sfruttare l'anno europeo della formazione per inserire, integrare e sviluppare quelle figure professionali specifiche che farebbero la differenza in tema di semplificazione, riorganizzazione e gestione, quali ad esempio il Chief Digital Officer e il Responsabile della conservazione.

IL RESPONSABILE DELLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI. INTERVISTA CON L’A.I.

Luigi Foglia

Abstract: tra i Professionisti della Custodia non può mancare il Responsabile della Conservazione dei documenti informatici (in inglese “Preservation Manager”) una figura professionale che affonda le sue radici nella tradizione giuridica e archivistica, incaricato di curare la conservazione e determinare la selezione della memoria digitale. Una figura cruciale in ambito pubblico e privato, ma quanto può dirsi conosciuta? L’Avv. Luigi Foglia intervista ChatGPT sul delicato ruolo del Responsabile della conservazione dei documenti informatici per capire dal web cosa veramente si sappia di questa professione e quali lacune siano ancora da colmare nell’accezione comune, posto che il settore dell’archiviazione digitale risulta ormai strategico per determinare ogni aspetto della nostra vita, presente e futura.

The Preservation Manager of electronic documents is a professional figure that has its roots in the legal and archival tradition, in charge of taking care of the preservation and determining the selection of the digital memory. A crucial figure in the public and private spheres, but how well known can it be? The lawyer Luigi Foglia interviews ChatGPT about the delicate role of the IT document preservation manager to understand from the web what is really known about this profession and what gaps still need to be filled in the common meaning, given that the digital archiving sector is now strategic for determining every aspect of our present and future life.

Parole chiave: responsabile – professione – documenti – conservazione - ChatGPT

Sommario: 1. Chi è il Responsabile della conservazione dei documenti informatici? 2. Di cosa è responsabile? - 3. Cosa deve fare un RdC per definire una politica di conservazione? - 4. Quali formati documentali consiglieresti per la conservazione dei documenti informatici? - 5. Per quanto tempo devo conservare una fattura? - 6. Quali devono essere le competenze del Responsabile della conservazione dei documenti informatici? - 7. Conclusioni

1. Chi è il Responsabile della conservazione dei documenti informatici?

Il Responsabile della conservazione dei documenti informatici (in inglese “Records Manager”) è un professionista che ha la responsabilità di gestire la creazione, la gestione, la conservazione e la distruzione dei documenti informatici all’interno di un’organizzazione. Questa figura lavora per garantire che i documenti informatici siano organizzati, accessibili, sicuri e conformi alle leggi e alle normative in materia di privacy e protezione dei dati. Il Responsabile della conservazione dei documenti informatici può lavorare all’interno del dipartimento IT o come parte di un’unità dedicata alla gestione dei documenti. In alcune organizzazioni, il Responsabile della conservazione dei documenti informatici è anche responsabile della gestione dei documenti cartacei.

2. Di cosa è responsabile?

Il Responsabile della conservazione dei documenti informatici è responsabile di molte attività importanti all’interno di un’organizzazione, tra cui:

1. Definire e implementare politiche e procedure per la gestione dei documenti informatici.
2. Assicurarsi che tutti i documenti siano archiviati in modo sicuro e accessibile per il tempo necessario.
3. Gestire la distruzione sicura dei documenti non più necessari.
4. Garantire la conformità alle leggi e alle normative in materia di privacy e protezione dei dati.
5. Gestire la classificazione e la catalogazione dei documenti informatici.
6. Assicurare la disponibilità e l’accessibilità ai documenti informatici per tutti coloro che ne hanno bisogno.
7. Collaborare con altre funzioni aziendali per garantire che i documenti informatici siano integrati nel flusso di lavoro e nelle operazioni aziendali.
8. Gestire eventuali richieste di accesso ai documenti informatici da parte di autorità pubbliche, tribunali o altri enti.
9. Formare e sensibilizzare il personale sulla gestione dei documenti informatici e sulle politiche e procedure aziendali in materia.
10. Monitorare e valutare continuamente le politiche e le procedure per garantire che siano adeguate e adeguate alle esigenze aziendali in evoluzione.

In sintesi, il Responsabile della conservazione dei documenti informatici è responsabile della gestione dei documenti informatici all’interno dell’organizzazione, comprese la creazione, la gestione, la conservazione e la distruzione dei documenti, la conformità alle leggi e alle normative, la classificazione e la catalogazione, la disponibilità e l’accessibilità e la collaborazione con altre funzioni aziendali.

3. Cosa deve fare un RdC per definire una politica di conservazione?

Per definire una politica di conservazione dei documenti informatici, è necessario considerare alcuni fattori importanti. Ecco un processo di base per la definizione di una politica di conservazione:

- **Definizione dei requisiti legali e normativi:** In primo luogo, è necessario comprendere le leggi e le normative che regolano la gestione dei documenti informatici, come la privacy e la protezione dei dati. Queste leggi definiscono il periodo di tempo per cui i documenti devono essere conservati e le condizioni per la loro distruzione.
- **Identificazione dei tipi di documenti da conservare:** È importante identificare i tipi di documenti che devono essere conservati, ad esempio contratti, fatture, rapporti, ecc. Questi documenti devono essere classificati in base alla loro importanza e alla loro sensibilità.
- **Definizione dei processi di creazione, gestione e distruzione dei documenti:** Dovrete stabilire procedure dettagliate per la creazione, la gestione e la distruzione dei documenti, compresi i requisiti per la sicurezza, la classificazione e la catalogazione.
- **Definizione degli standard di archiviazione:** Dovrete stabilire gli standard per la conservazione dei documenti, comprese le condizioni di sicurezza, la disponibilità e l'accessibilità. Questi standard dovrebbero essere in linea con le esigenze dell'organizzazione e con le leggi e le normative in materia di privacy e protezione dei dati.
- **Definizione dei ruoli e delle responsabilità:** Dovrete stabilire chi sarà responsabile delle attività di creazione, gestione e distruzione dei documenti, e definire le relative responsabilità.
- **Definizione dei processi di revisione e monitoraggio:** Dovrete definire i processi per la revisione e il monitoraggio della politica di conservazione, in modo da garantire che sia costantemente adeguata alle esigenze dell'organizzazione.
- **Comunicazione della politica di conservazione:** Infine, dovrete comunicare la politica di conservazione a tutti coloro che ne sono interessati all'interno dell'organizzazione, in modo che siano consapevoli dei loro ruoli e responsabilità.

4. Quali formati documentali consiglieresti per la conservazione dei documenti informatici?

Per la conservazione dei documenti informatici, è importante scegliere formati documentali che siano stabili, affidabili e aperti. Questo garantirà che i documenti siano accessibili e leggibili anche in futuro, anche se i software o i sistemi informatici utilizzati per crearli o visualizzarli cambieranno. Ecco alcuni dei formati documentali che si possono prendere in considerazione per la conservazione dei documenti informatici:

- **PDF/A:** è un formato di file PDF che è stato progettato specificamente per la conservazione a lungo termine. Questo formato garantisce che il documento sia visualizzato correttamente anche in futuro, indipendentemente dal software utilizzato per crearlo o visualizzarlo.
- **TIFF:** è un formato di file immagine che viene utilizzato comunemente per la conservazione dei documenti digitali. Questo formato è stabile e supporta una gamma di risoluzioni e profondità di colore.
- **XML:** è un formato di file che viene utilizzato comunemente per la conservazione di documenti strutturati, come ad esempio i metadati. Questo formato garantisce che i documenti siano facilmente accessibili e leggibili in futuro, indipendentemente dal software utilizzato per crearli o visualizzarli.
- **ODF:** è un formato di file aperto che viene utilizzato comunemente per la conservazione di documenti di testo, fogli di calcolo e presentazioni. Questo formato garantisce che i documenti siano facilmente accessibili e leggibili in futuro, indipendentemente dal software utilizzato per crearli o visualizzarli.

Questi sono solo alcuni esempi dei formati documentali che si possono utilizzare per la conservazione dei documenti informatici. La scelta del formato più adatto dipenderà dalle esigenze specifiche di ogni singolo caso. È importante tenere presente che i formati documentali dovrebbero essere scelti anche in base alla necessità di conservare eventuali metadati e di garantire la leggibilità dei documenti nel futuro.

5. Per quanto tempo devo conservare una fattura?

Il tempo di conservazione delle fatture varia a seconda delle leggi e delle norme fiscali vigenti nella giurisdizione in cui le fatture sono state emesse. In generale, le fatture devono essere conservate per un periodo di tempo sufficiente a soddisfare le esigenze fiscali e contabili, e per consentire la verifica delle transazioni commerciali in caso di controllo fiscale.

In Italia, ad esempio, le fatture devono essere conservate per dieci anni dalla data della loro emissione. Questo periodo di conservazione è stabilito dalla legge fiscale italiana e si applica a tutte le fatture emesse per operazioni effettuate sul territorio italiano.

È importante tenere presente che i requisiti di conservazione delle fatture possono variare a seconda delle leggi e delle norme fiscali vigenti nella giurisdizione specifica; quindi, è importante verificare le disposizioni fiscali locali per ottenere informazioni dettagliate sulle esigenze di conservazione delle fatture.

6. Quali devono essere le competenze del Responsabile della conservazione dei documenti informatici?

Il responsabile della conservazione dei documenti informatici deve possedere una serie di competenze per svolgere in modo efficiente e conforme alle leggi e alle norme il suo ruolo. Ecco alcune delle competenze che un responsabile della conservazione dei documenti informatici dovrebbe possedere:

Conoscenza delle leggi e delle norme relative alla protezione dei dati: il responsabile della conservazione dei documenti informatici deve conoscere e comprendere le leggi e le norme che regolamentano la protezione dei dati, come ad esempio il Regolamento Generale sulla Protezione dei Dati (RGPD) dell'Unione Europea.

Conoscenza dei sistemi informatici: il responsabile della conservazione dei documenti informatici deve avere conoscenze approfondite di sistemi informatici, reti e sicurezza informatica, per garantire che i documenti informatici siano adeguatamente protetti.

Conoscenza delle procedure di conservazione dei documenti: il responsabile della conservazione dei documenti informatici deve conoscere e comprendere le procedure e le pratiche relative alla conservazione dei documenti informatici, inclusa la classificazione, l'archiviazione, la gestione della dismissione e la protezione contro la perdita o il danneggiamento.

Abilità di problem solving: il responsabile della conservazione dei documenti informatici deve essere in grado di risolvere problemi tecnici e di sicurezza informatica in modo tempestivo e professionale.

Comunicazione: il responsabile della conservazione dei documenti informatici deve essere in grado di comunicare efficacemente sia con i dipendenti dell'azienda che con i rappresentanti di enti esterni, per garantire una corretta gestione dei dati.

Sensibilità verso la privacy: il responsabile della conservazione dei documenti informatici deve essere sensibile verso la privacy e la protezione dei dati personali, e adottare le misure appropriate per garantire che i dati siano trattati in modo sicuro e conforme alle leggi e alle norme applicabili.

7. Conclusioni

Animato da un forte curiosità, ho provato ad interrogare la ormai famosa Intelligenza Artificiale ChatGPT (ver. 30 gennaio 2023) e ho ottenuto delle risposte che, seppur non allineate alla normativa italiana e non in grado di rappresentare esaustivamente la complessità di alcuni dei temi trattati, risultano comunque coerenti, logiche e in molti casi un interessante punto di partenza per confrontarsi con la materia. Risulta evidente come l'A.I. interrogata prenda spunto da informazioni maggiormente legate al concetto (internazionalmente più diffuso) di *record management* e non a quello di *document management* a cui la nostra normativa si ispira; nonostante questo, le risposte ricevute sono in buona parte risultate ben al di sopra della conoscenza media dell'argomento (l'articolo riporta infatti una selezione delle più interessanti) che è possibile riscontrare nelle maggior parte delle aziende italiane. Al momento è quindi impossibile immaginare che un A.I. possa sostituire un essere umano nella propria attività, ma sicuramente un A.I. correttamente istruita e interrogata, già oggi potrebbe rappresentare un ottimo supporto per moltissimi processi decisionali.

IL RUOLO DEL RESPONSABILE DELLA TRANSIZIONE DIGITALE NELLA PROGETTAZIONE DI SERVIZI ON LINE

Sarah Ungaro

Abstract: Il Responsabile della transizione digitale è una figura ancora non del tutto compresa e valorizzata, sia in ambito pubblico, che privato. Eppure si tratta di un componente strategico del percorso di transizione digitale, incaricato di progettare e implementare i processi mediante un approccio olistico e in modo condiviso e trasversale con le altre figure apicali preposte al *management* e alla gestione dei diversi settori dell'organizzazione. Conosciamo da vicino le concrete declinazioni delle sue specifiche funzioni.

The Digital Transition Manager is a figure that is not yet fully understood and valued, both in the public and private sectors. Yet it is a strategic component of the digital transition path, in charge of designing and implementing processes using a holistic approach and in a shared and transversal way with the other top figures responsible for managing the various sectors of the organization. Let's see the concrete declinations of its specific functions.

Parole Chiave: transizione digitale – processi – innovazione – progettazione

Sommario: 1. Le molteplici responsabilità legate alla transizione digitale 2. Il contesto di riferimento e le possibili declinazioni 3. RTD: una figura chiave anche per l'utente finale 4. La progettazione di servizi on line per l'innovazione dei processi 5. Conclusioni

Il Responsabile della transizione digitale, in ambito pubblico o privato, ha un ruolo strategico, forse ancora non del tutto compreso e valorizzato.

Questa figura – altrimenti individuata anche nel Chief Digital Officer o nel Manager per la trasformazione digitale, nelle diverse organizzazioni - si occupa di coordinare la **progettazione e l'implementazione dei processi in ambito digitale**, mediante un approccio c.d. olistico e in modo condiviso e trasversale con le altre figure apicali preposte al *management* e alla gestione dei diversi settori dell'organizzazione.

L'espletamento di tale ruolo strategico implica – in primis – l'adozione delle **corrette competenze interdisciplinari**, nonché un'accurata **analisi e mappatura dei processi e delle relative fasi** (comprehensive degli attori che vi partecipano e degli eventuali fruitori degli stessi) che si intendono innovare e di cui incrementare l'efficienza, in un contesto – ovviamente - totalmente digitale.

1. Le molteplici responsabilità legate alla transizione digitale

Sotto il profilo delle funzioni specifiche da esercitare, il ruolo del Responsabile della transizione digitale comporta molteplici responsabilità, tra cui:

1. Definizione della strategia digitale: aiuta a definire la visione, gli obiettivi e la strategia digitale dell'organizzazione.
2. Valutazione delle tecnologie: valuta le tecnologie più adatte alle esigenze dell'organizzazione e ne supporta l'implementazione.
3. Coordinamento delle attività: coordina le attività in relazione all'innovazione dei processi, in chiave totalmente digitale, all'interno dell'organizzazione per garantirne la condivisione e la trasversalità.
4. Gestione dei progetti per l'innovazione digitale dei processi: gestisce progetti, assicurandosi che vengano completati in modo tempestivo e in budget.
5. Formazione del personale: supporta la formazione del personale sulla gestione di dati e documenti in ambito digitale, sulla protezione dei dati personali e sulla sicurezza informatica per garantirne la competenza.
6. Sensibilizzazione interna ed esterna sull'attenzione ai progetti di innovazione digitale: supporta la comunicazione interna ed esterna per promuovere la consapevolezza e la sensibilizzazione di personale, utenti, clienti e partner sui temi dell'innovazione digitale dei processi dell'organizzazione.

Delle concrete declinazioni di tali specifiche funzioni se ne è parlato durante il **Forum Nazionale sulla custodia dei contenuti digitali¹**, organizzato da ANORC nel mese di ottobre 2022.

2. Il contesto di riferimento e le possibili declinazioni

Come emerso anche durante il Forum ANORC, se nel contesto di un'azienda o un'organizzazione privata il Responsabile della transizione digitale ha generalmente un ruolo di coordinamento tra le diverse divisioni aziendali in relazione alla pianificazione e all'implementazione dei diversi processi di innovazione digitale e considerando che tale ruolo può essere concretamente declinato in modo diverso, in base all'organizzazione di riferimento e agli obiettivi aziendali di volta in volta fissati; diversamente, nell'ambito di una Pubblica Amministrazione, il Responsabile della transizione digitale è una figura i cui numerosi e complessi compiti sono espressa-

¹ <https://anorc.eu/attivita/anorc-presenta-il-forum-nazionale-sulla-custodia-dei-contenuti-digitali-tre-giornate-dedicate-a-dpo-rdc-e-rtd/>

mente elencati **nell'art. 17 del CAD²** (Codice dell'Amministrazione Digitale, di cui al D.Lgs. n. 82/2005).

Risulta utile notare, in proposito, che è la stessa norma – al comma 1-ter – a precisare che il Responsabile della transizione digitale “è dotato di adeguate **competenze**

² D.Lgs. n. 82/2005, art. 17 (Responsabile per la transizione digitale e difensore civico digitale):

1. Le pubbliche amministrazioni garantiscono l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo in coerenza con le Linee guida. A tal fine, ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità. Al suddetto ufficio sono inoltre attribuiti i compiti relativi a:

- a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
- b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
- c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
- d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
- e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
- f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
- g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
- h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
- i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
- j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis.
- j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.

1-ter. Il responsabile dell'ufficio di cui al comma 1 è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione, alla modalità digitale direttamente all'organo di vertice politico.

(*omissis*).

1-sexies. Nel rispetto della propria autonomia organizzativa, le pubbliche amministrazioni diverse dalle amministrazioni dello Stato individuano l'ufficio per il digitale di cui al comma 1 tra quelli di livello dirigenziale oppure, ove ne siano privi, individuano un responsabile per il digitale tra le proprie posizioni apicali. In assenza del vertice politico, il responsabile dell'ufficio per il digitale di cui al comma 1 risponde direttamente a quello amministrativo dell'ente.

1-septies. I soggetti di cui al comma 1-sexies possono esercitare le funzioni di cui al medesimo comma anche in forma associata.

tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale direttamente all'organo di vertice politico”.

In effetti, la necessità del possesso di tali articolate competenze – indicate *ex lege* - in capo a questa figura risulta in linea con la scelta del Legislatore di individuare tendenzialmente **un ufficio dirigenziale generale per la transizione digitale**, il cui staff sia coordinato da un Responsabile.

Tra i compiti menzionati all'art. 17 del CAD rientra anche la **progettazione e il coordinamento** delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese.

3. RTD: una figura chiave anche per l'utente finale

Proprio su questo tema, in relazione ai servizi digitali erogati online, il Responsabile della transizione digitale ha un ruolo chiave nella definizione degli obiettivi e delle strategie per **migliorare l'esperienza degli utenti, la sicurezza dei dati e l'efficienza dei processi online**, supervisionando la selezione e l'implementazione delle tecnologie e degli strumenti necessari per offrire servizi digitali di alta qualità e integrati con gli altri processi dell'amministrazione di riferimento.

Il Responsabile della transizione digitale **ha il compito di gestire e coordinare l'implementazione dei servizi digitali erogati on-line da un sito web**, al fine di garantirne la fruibilità e l'efficacia. Ciò può includere attività come lo sviluppo e l'aggiornamento del sito web, la gestione dei dati degli utenti e la sicurezza informatica, la valutazione e l'adozione di tecnologie innovative, nonché la promozione e la comunicazione dei servizi digitali offerti. In sostanza, il responsabile della transizione digitale si occupa di **assicurare che i servizi digitali erogati on-line da un sito web siano accessibili, sicuri, user-friendly e conformi alle normative vigenti**, adottando un approccio c.d. user-centric, improntato al soddisfacimento delle esigenze degli utenti.

Nello specifico, il riferimento agli utenti non è solo da intendersi a coloro i quali usufruiscono di tali servizi on line, ma **anche a coloro che in qualche modo ne gestiscono i relativi processi nel back office**.

Tale nuovo approccio all'e-government comporta che gli obiettivi della trasformazione digitale dei servizi pubblici siano volti a:

- **invertire il punto di vista burocratico** - quello in cui il focus della progettazione è l'istituzione – prediligendo invece un approccio che parte dai bisogni dell'utente, il cittadino in primis;
- **non dimenticare chi sia l'utente** di qualsiasi sistema funzionale all'erogazione di un servizio, tanto quello finale, il cittadino, quanto il tecnico della Pubblica Amministrazione che progetta, implementa o opera nel quotidiano il servizio stesso.

4. La progettazione di servizi on line per l'innovazione dei processi

Questo aspetto è chiarito espressamente proprio nelle recenti **Linee guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione**, adottate da AgID con la determina del 27 luglio n. 224/2022, affiancate dal relativo Manuale operativo (del 23 gennaio 2023), che contengono utilissime indicazioni per i Responsabili della transizione digitale e per tutti coloro che sono coinvolti nella progettazione di servizi on line e nelle attività che implicano nuove analisi e valutazioni per l'innovazione dei processi in un contesto digitale.

Questi i principi guida indicati da AgID in tema di servizi on line:

- digital & mobile first (digitale e mobile come prima opzione): le pubbliche amministrazioni devono realizzare servizi primariamente digitali;
- digital identity only (accesso esclusivo mediante identità digitale): le pubbliche amministrazioni devono adottare in via esclusiva sistemi di identità digitale definiti dalla normativa;
- cloud first (cloud come prima opzione): le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in;
- servizi inclusivi e accessibili: le pubbliche amministrazioni devono progettare servizi pubblici digitali che siano inclusivi e che vengano incontro alle diverse esigenze delle persone e dei singoli territori;
- dati pubblici un bene comune: il patrimonio informativo della pubblica amministrazione è un bene fondamentale per lo sviluppo del Paese e deve essere valorizzato e reso disponibile ai cittadini e alle imprese, in forma aperta e interoperabile;
- interoperabile by design: i servizi pubblici devono essere progettati in modo da funzionare in modalità integrata e senza interruzioni in tutto il mercato unico esponendo le opportune API;
- sicurezza e privacy by design: i servizi digitali devono essere progettati ed erogati in modo sicuro e garantire la protezione dei dati personali;
- user-centric, data driven e agile: le amministrazioni sviluppano i servizi digitali, prevedendo modalità agili di miglioramento continuo, partendo dall'esperienza dell'utente e basandosi sulla continua misurazione di prestazioni e utilizzo;
- once only: le pubbliche amministrazioni devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite;
- transfrontaliero by design (concepito come transfrontaliero): le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti;
- codice aperto: le pubbliche amministrazioni devono prediligere l'utilizzo di software con codice aperto e, nel caso di software sviluppato per loro conto, deve essere reso disponibile il codice sorgente.

5. Conclusioni

Sulla scorta di questi principi guida, risulta più facile comprendere che il Responsabile della transizione digitale deve essere in grado di **progettare, realizzare e governare tali nuovi processi non curandosi esclusivamente degli aspetti tecnologici**, ma valorizzando nuovi paradigmi di organizzazione e logiche procedurali innovative, che devono essere sottese alla trasformazione in chiave digitale di un determinato servizio.

SEZIONE I
L'EVOLUZIONE DIGITALE DEGLI ARCHIVI

IL RUOLO DELLA CONSERVAZIONE NEL PROCESSO DI DIGITALIZZAZIONE DEL PAESE

Patrizia Gentili

Abstract: Cosa si intende per conservazione? È di fatto la funzione in grado di assicurare che gli utenti del futuro possano identificare, ricercare, trattare, interpretare, utilizzare documenti digitali in un ambiente caratterizzato dalla modifica costante della tecnologia e in condizioni che assicurino la presunzione di autenticità dei documenti stessi.

Questo richiede la gestione del rischio di perdita dei dati e l'aggiornamento continuo delle regole e della tecnologia per far fronte all'obsolescenza.

Conservare pertanto è la capacità di riprodurre nel tempo e implica innovazione, responsabilità, documentazione e... archivisti.

Conservare bene significa quindi massima attenzione all'organizzazione: da qui discende l'obbligo del manuale di conservazione e una precisa definizione dei compiti del responsabile della conservazione.

Nell'articolo si approfondiranno questi temi e questi strumenti, indispensabili per rispondere alle esigenze di una conservazione di qualità.

What do we mean by preservation? It is the task able to ensure to the future users the identification, search, treatment, understanding, employ of digital documents in such conditions that ensure the presumption of validity.

All this happens in an environment characterized by technological rapid evolution, the need to effectively manage the risk of data loss and the continuous updating of the rules.

Preserving therefore is the ability to reproduce documents over time and implies innovation, responsibility, documentation and ... archivists.

Preserving well means paying the highest attention to organizational profiles: consequently we have the duty of the preservation manual and precisely defined tasks of the preservation manager.

This article will completely examine these issues, the full comprehension of is a crucial requirement for answering to the needs of quality preservation.

Parole chiave: conservazione – archivi – archivisti – documenti – compiti – responsabilità - innovazione

Sommario: 1. Introduzione – 2. Le criticità – 3. Le soluzioni – 4. Il riversamento – 5. Gli Strumenti – 6. Il Manuale di Conservazione – 7. Il Responsabile della Conservazione – 8. Alcune buone pratiche di conservazione – 9. Le architetture – 10. Conclusioni.

1. Introduzione

L'importanza del processo di memorizzazione dei documenti digitali è sempre più cruciale in un contesto di digitalizzazione ormai avviato e che ha per obiettivi l'accesso, l'integrità e l'autenticità nel tempo dei documenti amministrativi informatici. Il processo di conservazione diventa così strategico per la pubblica amministrazione impegnata nell'innovazione del Paese.

Le buone pratiche di conservazione applicate da alcune amministrazioni centrali e locali ci permettono oggi di comprendere efficacemente l'applicazione di quanto la normativa di settore impone.

Ma come possiamo definire il concetto di conservazione ed evitare fraintendimenti? Esistono molteplici esempi di definizioni, ma quella che sicuramente meglio riassume i concetti fondamentali è, a mio parere, la seguente:

*“L'insieme dei **principi**, delle **politiche**, delle **disposizioni** e delle **strategie finalizzate a prolungare l'esistenza di un documento o di una risorsa digitale grazie alla sua tenuta in condizioni adatte all'uso nella forma originale e/o in un formato persistente che garantisca l'integrità della configurazione logica e del contenuto**”.*

È quindi l'attività volta a proteggere e custodire nel tempo gli archivi di documenti e dati informatici. Le parole chiave su cui concentrare l'attenzione sono: autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti nel tempo.

2. Le criticità

La conservazione di fatto si basa su attività di **prevenzione** e **manutenzione**. Prevenzione nel senso di limitazione del rischio di perdita di informazioni, manutenzione nell'ottica di una continua verifica delle condizioni di integrità, efficienza funzionale e identità degli archivi.

Nel progettare un sistema di conservazione che risponda al dettato normativo si deve avere piena coscienza delle criticità che a vari livelli sono insite nella tematica. Innanzitutto, dato che i documenti digitali necessitano di un supporto sul quale essere memorizzati, uno dei problemi più frequenti è dato proprio dalla **obsolescenza dei supporti** utilizzati.

Ma, considerando che i documenti digitali sono costituiti da bit e che per essere letti hanno bisogno di un «formato» che riconosca la codifica con la quale sono stati prodotti (word, excel, pdf, tiff, jpeg, mp3, avi...), anche l'**obsolescenza dei formati** diventa un punto di attenzione.

Infine, dato che i documenti informatici per poter essere letti hanno bisogno di una piattaforma e di strumenti tecnologici, abbiamo il rischio dell'**obsolescenza tecnologica**.

Ricordiamo che la pubblica amministrazione è soggetta a obblighi molto stringenti in considerazione del fatto che tutti i suoi documenti e archivi sono protetti e tutelati

dal Codice dei beni culturali in attuazione dell'articolo 9 della carta costituzionale. La tutela riguarda tutte le attività finalizzate ad assicurare o a minacciare la persistenza dei patrimoni documentari di natura pubblica e implica il rispetto dei principi e dei metodi che garantiscono la conservazione nel tempo degli archivi (documenti e, soprattutto, aggregazioni).

3. Le soluzioni

Ognuna delle problematiche sopra evidenziate implica una serie di comportamenti e pratiche ben strutturati. Si deve cioè definire minuziosamente politiche e requisiti funzionali del sistema di conservazione in conformità con la normativa vigente, con gli standard internazionali e in conformità con la specificità degli oggetti da conservare (inclusa la loro natura archivistica).

Ma in concreto cosa si deve fare?

Quando si parla di obsolescenza del supporto e di obsolescenza dei formati l'unica soluzione possibile è il **riversamento**. Ma prima di affrontare questo tema dobbiamo premettere che una delle attività essenziali correlate ad una corretta gestione documentale è la cosiddetta "*valutazione di interoperabilità*".

Per effettuarla, le amministrazioni devono attuare una ricognizione di tutte le proprie procedure amministrative e/o processi di business, per individuare ogni tipologia di documenti informatici trattati (o trattabili). Attraverso la ripetizione della valutazione di interoperabilità ad intervalli regolari divengono evidenti i formati in via di obsolescenza (quando non già conservati in un formato obsoleto), permettendo quindi di pianificare proattivamente le necessarie azioni di contrasto, tra cui proprio il riversamento di cui parleremo nel paragrafo seguente.

Per quanto attiene al rischio di obsolescenza tecnologica, l'unica soluzione è prevedere un continuo aggiornamento mediante percorsi di formazione attentamente pianificati al fine di rispondere sempre alle continue evoluzioni cui il mondo digitale è soggetto. Tutti i processi dell'innovazione, infatti, sono pervasi dal tema delle competenze digitali come acceleratore delle loro fasi e rappresentano il comune denominatore per un approccio consapevole e qualificato al fine di un consolidamento del processo di cambiamento guidato dalle moderne tecnologie. Le competenze digitali esercitano quindi un ruolo fondamentale e rappresentano un fattore abilitante.

4. Il riversamento

Il riversamento di formato comporta il trasferimento di un documento informatico in un formato di file diverso: contestualmente, ciò può comportare anche una duplicazione da un supporto ad un altro (volume, disco, nastro, filesystem, storage ad oggetti o altri). Per quanto già detto, le strategie relative alla gestione dei formati e

dei supporti vanno spesso di pari passo; perciò, in alcuni casi può essere operativamente ed economicamente vantaggioso effettuare i riversamenti di formato contestualmente a quelli di supporto. I riversamenti vengono pianificati a seguito di una nuova valutazione di interoperabilità, considerando i costi e i benefici di una tale operazione.

Quando si effettua un riversamento finalizzato alla conservazione, il file riversato è una copia digitale di un documento originale e, come tale, la conformità della copia deve essere attestata in base alla normativa vigente.

Il riversamento di un formato deve essere effettuato mediante un processo certificato che ne garantisca l'integrità e la riproducibilità. Ogni procedura di riversamento è descritta nel manuale di gestione. Per le pubbliche amministrazioni ovviamente il riversamento deve avvenire sempre in formati che ne migliorano l'interoperabilità.

5. Gli strumenti

Conservare, come detto, è la capacità di riprodurre nel tempo la conservazione digitale e implica innovazione, responsabilità, documentazione e ... archivisti. Una conservazione di qualità significa una grande enfasi sull'organizzazione e da qui discende l'obbligo del manuale di conservazione e una precisa definizione dei compiti del responsabile della conservazione.

Questi due strumenti organizzativi riducono la discrezionalità degli interventi, accrescono gli strumenti di verifica e le garanzie di auditing accurati.

A questo si aggiunge che nel tempo sono stati definiti una serie di profili professionali legati alle attività di conservazione, proprio con lo scopo di garantire una conservazione di qualità.

6. Il manuale di conservazione

Il manuale di conservazione costituisce la base essenziale per garantire e documentare a fini giuridici e a fini di ricerca storica le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

Illustra dettagliatamente l'organizzazione, i soggetti coinvolti nelle attività di conservazione e i loro ruoli, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il manuale di conservazione è un documento obbligatorio anche per i privati che conservano i propri documenti in modalità informatica e riguarda l'individuazione delle tipologie documentali trattate e dei relativi metadati da associare, le modalità e i tempi di trasmissione dei pacchetti di versamento e le tempistiche di selezione e

scarto dei propri documenti informatici.

Dobbiamo immaginare il manuale come un contenitore che racchiude tutto il processo che riguarda la conservazione dei documenti informatici di un'organizzazione. Pertanto, al suo interno sarà necessario descrivere le attività del personale coinvolto in questo processo, le tipologie documentali trattate dall'organizzazione (fatture, documenti di trasporto, mail, PEC e altre ancora) e con quali modalità queste vengono prodotte e conservate per far sì che si garantiscano i criteri di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Nel dettaglio il manuale deve contenere almeno:

- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema;
- la struttura organizzativa;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione;
- la descrizione delle modalità di presa in carico dei pacchetti di versamento e generazione del rapporto di versamento;
- la descrizione del processo di conservazione dei pacchetti di archiviazione;
- la modalità di produzione del pacchetto di distribuzione;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi;
- la descrizione delle procedure per la produzione di duplicati o copie;
- i tempi entro i quali le diverse tipologie di documenti devono essere scartate o trasferite in conservazione qualora, nel caso delle pubbliche amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
- le modalità con cui viene richiesta la presenza di un pubblico ufficiale.

7. Il responsabile della conservazione

Per redigere il manuale di conservazione si devono possedere adeguate competenze archivistiche, informatiche e gestionali. Ogni pubblica amministrazione deve identificare una figura che le posseda tutte: il Responsabile della Conservazione, nominato obbligatoriamente internamente.

Per le aziende private, invece, questa figura può anche essere demandata all'esterno, purché naturalmente non coincida con il conservatore, qualora ci si avvalga di un servizio di conservazione in outsourcing.

Il Manuale della Conservazione, quindi, deve essere redatto dal Responsabile della Conservazione.

8. Alcune buone pratiche di conservazione

Nell'ambito dei lavori sui Poli di conservazione sono state riscontrate almeno tre tipologie di Poli di conservazione già in essere:

- quella relativo alla conservazione permanente (Archivio Centrale dello Stato - ACS);
- quella relativo ad amministrazioni centrali (Consiglio nazionale del Notariato, Agenzia Industrie Difesa - CEDECU e SOGEI);
- quella relativa a realtà territoriali (Polo archivistico dell'Emilia-Romagna - PARER, Regione autonoma Friuli-Venezia Giulia, Polo Marche DIGIP - Regione Marche, e Centro archivistico Regione Veneto - POLARC).

Laddove il Polo ACS presenterà una sua specificità rispetto alle altre tipologie di poli di conservazione in quanto, per mandato istituzionale, è destinato a **conservare permanentemente** gli archivi digitali storici di diversa provenienza statale, gli altri poli, in aggiunta alla loro missione principale, sviluppano anche servizi e progetti interregionali e con enti nazionali, condividendo esperienze, soluzioni applicative e piattaforme tecnologiche proprie dei sistemi di conservazione.

9. Le architetture

Le architetture dei sistemi di conservazione utilizzate presso questi poli condividono soluzioni informatiche e tecnologiche moderne (a componenti modulari, a micro-servizi, caratterizzate da forte scalabilità ed elevata sicurezza, orientate al web, etc.). Sono però inevitabilmente eterogenee sia in ragione del mandato istituzionale di ciascuno, sia in considerazione del volume di transazioni giornaliere da sostenere, dei tempi prevalenti di conservazione dei documenti e della loro tipologia, dei livelli di sicurezza e di altri parametri gestionali.

Abbiamo quindi architetture molto complesse quali quelle di Sogei e PARER ma anche architetture più semplici quali quelle di CEDECU, Digip della Regione Marche e POLARC della Regione Veneto che offrono servizi all'utenza mediante applicazioni web. La soluzione di POLARC però, a differenza degli altri poli, non gestisce in proprio la conservazione documentale ma opera in logica di Hub offrendo ai suoi utenti, mediante un'interfaccia web unificata, i servizi di conservazione acquisiti da conservatori esterni, anche essi interagenti mediante una loro specifica interfaccia web.

10. Conclusioni

Perché la conservazione dei documenti è così importante? Perché è di fatto una attività essenziale insita nella produzione documentale stessa e per le pubbliche amministrazioni rappresenta un compito istituzionale, sia come testimonianza diretta

delle proprie azioni al servizio della collettività sia come memoria storica.

L'obbligo di conservazione dei documenti d'archivio è inteso a salvaguardare diritti soggettivi, interessi legittimi, il diritto d'accesso, la ricerca a fini storici, culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico.

L'aumento esponenziale della mole di documenti digitali, causata dalla spinta continua del legislatore verso il paperless office, comporta una priorità assoluta: **conservare bene**. È un'attività infatti che, se non bene governata, potrebbe portare nel medio e lungo termine alla perdita di informazioni essenziali.

Per la normativa italiana, come già detto, gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico sono **beni culturali *ab origine***, così come gli archivi e i singoli documenti, appartenenti a privati, che rivestono interesse storico particolarmente rilevante.

...E questa è la differenza sostanziale con il resto dei paesi europei.

GLI ARCHIVISTI

E LA CONSERVAZIONE DEGLI ARCHIVI DIGITALI

Micaela Procaccia

Abstract: Una corretta conservazione di documenti informatici, che ne garantisca leggibilità e autenticità nel tempo implica anche la conservazione della struttura e dei legami logici e di contesto che ne hanno determinato l'articolazione. Gli archivi digitali hanno fatto emergere con evidenza la necessità imprescindibile di progettare fin dalla nascita dell'archivio gli indispensabili strumenti di governo della documentazione, in estrema sintesi, il combinato fra i tradizionali strumenti archivistici e le soluzioni tecniche che possano garantirne i requisiti di accuratezza, integrità, affidabilità, leggibilità, nel corso del tempo. A maggior ragione, se si considera che una parte di questi archivi (e dunque anche documenti e relativi contenuti) se pubblica o se privata di riconosciuto interesse storico, sarà oggetto di una conservazione a lungo termine il cui scopo non sarà più quello della gestione amministrativa ma quello della ricerca storica. La responsabilità di individuare tempi di conservazione e modalità di transito ad una ambiente di conservazione di lungo termine non può che essere degli archivisti, ossia preparare scientificamente la delicatissima operazione dello scarto. Le esperienze maturate negli ultimi anni, in particolare in relazione alla cospicua documentazione digitale prodotta dagli archivi di impresa e dagli archivi degli architetti non ha fatto che confermare lo stretto legame tra progettazione, gestione e conservazione di un archivio digitale, sottolineando l'importanza del ruolo degli archivisti in tutte le fasi.

Correct conservation of electronic documents, which guarantees their legibility and authenticity over time, also implies the conservation of the structure and of the logical and contextual links that determined their articulation. Digital archives have clearly brought out the essential need to design the indispensable documentation management tools right from the very beginning of the archive, in a nutshell, the combination of traditional archival tools and the technical solutions that can guarantee the accuracy requirements, integrity, reliability, readability, over time. Moreover, if one considers that a part of these archives (and therefore also documents and related contents) if public or private of recognized historical interest, will be subject to long-term conservation whose purpose will no longer be that of administrative management but that of historical research. The responsibility for identifying conservation times and methods of transit to a long-term conservation environment can only rest with the archivists. The experiences gained in recent years, in particular in relation to the conspicuous digital documentation produced by company archives and architects' archives, has only confirmed the close link between design, manage-

ment and conservation of a digital archive, underlining the importance of the role of archivists at all stages.

Parole chiave: archivi digitali, archivisti, conservazione, conservazione di lungo termine, imprese, studi di progettazione.

Sommario: 1. Premessa: possiamo parlare solo di conservazione? – 2. Il ruolo degli archivisti – 3. Conclusioni e auspici: archivisti nella nuvola.

1. Premessa: possiamo parlare solo di conservazione?

Vorrei iniziare con una domanda, forse un po' provocatoria, che investe il tema stesso indicato per questa raccolta di saggi: è lecito, in riferimento alla produzione di contenuti documentari digitali, separare il concetto di "conservazione" dai concetti di produzione, descrizione, archiviazione e fruizione? A monte di questa domanda c'è una riflessione ormai quasi ovvia, almeno per gli archivisti, ma – tanto per fare un esempio – in qualche misura anche per l'AgID e per tutti i suoi predecessori a partire dagli anni '90, CNIPA, Digit PA e via dicendo, dal momento che gli archivisti sono stati chiamati a partecipare a tutti i tavoli di lavoro che si proponevano di dettare indicazioni, regole, linee guida per l'informatizzazione delle pubbliche amministrazioni: non si gestiscono, nel campo della produzione documentaria, i "contenuti" digitali di documenti digitali, ma documenti digitali ed i loro contenuti e, più correttamente, fascicoli informatici, e aggregazioni documentali informatiche che costituiscono archivi.

«Un dato non assume alcun significato se non è valorizzato da altri dati che lo descrivono (metadati) e lo contestualizzano. In un minuto lo spiega il comandante Ed Straker, in un telefilm cult del 1970». https://www.youtube.com/watch?v=fKxJ_0TGtoE» (Gianni Penzo Doria, PROCEDAMUS - UFO il significato dei dati - YouTube).

Non è una precisazione da poco, perché rinvia alla necessità di gestire questi insiemi documentari mantenendone le reciproche relazioni e progettandone la conservazione anche in vista di un lungo termine che afferisce alla loro natura di testimonianza storica, o di "memoria", come sempre più si dice, anche per comunicare la mutevolezza nel tempo dei concetti e la loro natura di relazione fra soggetti diversi. I conservatori e i fruitori *in primis*¹. E mette appena conto ricordare che è la stessa normativa vigente a considerare (articolo 10, comma 2, lettera *b* del D.lgs. 42/2004, Codice dei beni culturali e del paesaggio) non scindibili le fasi del ciclo di vita di un archivio, quando – nel definire cosa sia un bene culturale – recita: «Sono inoltre beni culturali [...] gli archivi e i singoli documenti dello Stato, delle regioni, degli altri

¹ Vedi in particolare, S. Vitali, *Di angeli, di paperi e di conigli, ovvero dello strano mestiere dell'archivista*, in «Professione: archivista»: 1949-1999. I cinquant'anni dell'ANAI nel mondo archivistico, Atti del convegno di studi (Trento-Bolzano, 24-26 novembre 1999), «Archivi per la storia», XIV/1-2 (2001), pp. 179-186

enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico» senza alcun riferimento alla loro lontananza nel tempo.

La buona conservazione di un archivio (analogico, certo, ma soprattutto digitale) non può essere scissa dalla sua produzione, gestione e conservazione.

«Il documento digitale...non ci dà tempo e se non mettiamo le premesse per la sua conservazione nel momento della formazione ha una vita brevissima. Per consentire una sua trasmissione alle prossime generazioni dobbiamo quindi essere in grado di agire velocemente e di operare scelte gestionali spesso sfidanti e di forte impatto organizzativo sulle nostre strutture»²

È, ancora una volta, una considerazione ormai scontata, che se un archivio cartaceo è comunque recuperabile pur in stato di disordine (ma questo disordine incide comunque sulla efficienza di chi lo ha prodotto, quanto meno in termini di reperibilità dei documenti) un archivio digitale non correttamente archiviato non sarà facilmente utilizzabile e perderà parte del suo valore contenutistico quando privato dei suoi riferimenti e legami interni. Come si diceva nel linguaggio tradizionale, quando perde il suo “vincolo archivistico” che conferisce senso al contesto che è sempre fatto di un legame fra domande e risposte, fra decisione e attuazione, fra esigenza e soddisfazione della stessa e via dicendo, in un contesto che solo da pieno senso al singolo documento. Recitava uno spiritoso post di qualche anno fa, pubblicato il giorno di San Valentino dagli *Archivisti in movimento*, «L'amore dura un sospiro, il vincolo archivistico è per sempre».

E il discorso vale certamente anche per qualunque archivio, non solo quelli delle pubbliche amministrazioni, se un recente volume dedicato agli archivi di impresa (archivi in gran parte privati e fortemente condizionati dalle modalità contemporanee, dunque digitali, di produzione documentaria³) dedica ampio spazio in diversi saggi al tema.

«Il tema della creazione, laddove possibile, dell'unità archivistica nel momento della formazione dei documenti non è irrilevante anche ai fini della conservazione dell'archivio in ambiente digitale. Qualunque archivistica sa bene che gestire singoli documenti o interi fascicoli fa molta differenza soprattutto nel momento in cui si voglia procedere alla selezione, che è il principio di qualunque tipo di conservazione, in una prospettiva storica, con buona pace di chi ritiene inutile lo scarto in ambiente informatico, grazie alla presenza di memorie sempre più grandi e motori di ricerca sempre più raffinati e potenti. È pur vero che procedere allo scarto di singoli documenti senza aver stabilito regole di conservazione nel momento della loro produzione come parti di unità archivistiche (le bozze di un fascicolo editoriale) o intere serie

² B. Costa, *Ritorno al futuro: tecnologia, sostenibilità, condivisione. Alcune lezioni apprese dall'esperienza*, in *Archivi d'impresa. Archivisti, storici, heritage manager di fronte al cambiamento*, a cura di G. Bonfiglio Dosio, C. Lussana, L. Nardi, Edizioni ANAI, Roma 2020, pp.371-380. La citazione è a p. 373. L'autrice fa riferimento all'esperienza nell' archivio storico di Intesa San Paolo di cui è responsabile.

³ *Archivi d'impresa. Archivisti, storici, heritage manager di fronte al cambiamento*, cit.

archivistiche è faticoso e, dal punto di vista informatico, apparentemente inutile»⁴. La determinazione dei criteri delle procedure dello scarto e dei tempi di conservazione è una operazione di alto contenuto intellettuale e che implica una assunzione di responsabilità nei confronti delle future generazioni tutt'altro che indifferente.

2. Il ruolo degli archivisti

Da quanto sopra richiamato, emergono alcune conseguenze: una corretta conservazione di documenti informatici, che ne garantisca leggibilità e autenticità nel tempo implica anche la conservazione della struttura e dei legami logici e di contesto che ne hanno determinato l'articolazione. Gli archivi digitali hanno fatto emergere con evidenza la necessità imprescindibile di progettare fin dalla nascita dell'archivio gli indispensabili strumenti di governo della documentazione, in estrema sintesi, il combinato fra i tradizionali strumenti archivistici (titolario di classificazione, piano di conservazione e scarto, manuale di gestione e regolamento) e le soluzioni tecniche che possano garantirne i requisiti di accuratezza, integrità, affidabilità, leggibilità, nel corso del tempo. Ciò è reso ancora più indispensabile dalla considerazione che una parte di questi archivi (e dunque anche documenti e relativi contenuti) se pubblica o se privata di riconosciuto interesse storico, sarà oggetto di una conservazione a lungo termine il cui scopo non sarà più quello della gestione amministrativa ma quella della ricerca storica. La responsabilità di individuare tempi di conservazione e modalità di transito ad una ambiente di conservazione di lungo termine non può che essere degli archivisti. E questo compito, la cui rilevanza non sfugge, è stato riconosciuto anche da AgID con la scelta, nel «Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici» di non fornire nelle disposizioni su requisiti e specifiche afferenti a forniture di servizi di conservazione per gli archivi digitali storici che dovranno essere invece conformi alle indicazioni che potranno essere emanate dalle competenti autorità archivistiche. E, tuttavia, appare evidente che gli archivisti non possono che essere presenti fin dall'inizio del processo di produzione e gestione dei documenti digitali.

Va anche ricordato che l'inserimento stesso del documento in una catena di "ininterrotta custodia", certificata dal suo essere parte di un sistema documentale è una delle garanzie di autenticità nel tempo del documento stesso.

«...per costruire sistemi logici integrati e procedure complessive di gestione documentale è importante che nelle imprese operi una figura intermedia tra chi produce e chi si occupa degli aspetti informatici: un intermediario competente, capace di promuovere e contemperare esigenze apparentemente contrastanti di rapidità e qualità delle informazioni gestite nell'operatività quotidiana e di archiviazione e conserva-

⁴ A. Bilotto, M. Guercio, *Problemi e prospettive: uno sguardo al futuro*, in *Archivi d'impresa Archivisti, storici, heritage manager di fronte al cambiamento*, cit. pp. 411-421, la citazione è a p. 415.

zione della memoria...»⁵.

Le tipologie di archivi ora all'attenzione dei professionisti e il tema della loro conservazione pongono problemi presenti da tempo anche in archivi analogici ma ora decisamente in primo piano: come, ad esempio, la molteplicità di tipologie documentali presenti negli archivi delle costruzioni o negli archivi delle imprese in generale, dal progetto non più disegnato ma realizzato in modalità BIM o la presenza negli archivi di impresa di oggetti digitali in 3D. Se la conservazione e reperibilità nel tempo va progettata dall'inizio, il ruolo degli archivisti deve intervenire sin da questa fase e non limitarsi al momento per così dire "conclusivo" della vita del documento destinato alla conservazione nel tempo.

La recente esperienza (ancora in corso) del gruppo di lavoro ANAI dedicato agli archivi digitali del settore delle costruzioni ha dato luogo a una serie di interessanti riflessioni. Nato su sollecitazione di alcuni studi di progettazione e di alcuni architetti il gruppo ha analizzato le diverse tipologie documentarie che ne caratterizzano l'attività e le criticità sorte con l'adozione di sistemi di produzione digitale dei documenti. «Tenere sotto controllo la produzione documentale dello studio equivale a produrre un lavoro di qualità e a salvaguardare diritti soggettivi dello studio, dei vari collaboratori e dei committenti. Gestire bene l'archivio di lavoro costituisce un valore aggiunto rispetto al buon esito dell'attività progettuale, comprendente il benessere di chi lavora e la soddisfazione del cliente, ed è perfino un fattore non trascurabile di marketing per lo studio»⁶.

La difficoltà di ricondurre ad un insieme coerente di documenti reperibili e conservati in modo da essere utilizzabili nel tempo, siano essi documenti giuridicamente necessari (dai bilanci ove necessari alla documentazione di deposito dei brevetti) o documenti di vera e propria progettazione in cui coesistono supporto analogico e supporto digitale tramite l'utilizzo di software assai diversi, e tutti di fondamentale importanza per i professionisti in una prospettiva di conservazione a lungo termine, ha richiesto, soprattutto per il crescente uso di documentazione digitale, «una pianificazione rigorosa e di un funzionamento rigidamente regolamentato del sistema documentale nel suo complesso. Peraltro il digitale consente aggregazioni impensabili con l'analogico: basti pensare alla possibilità di includere nel medesimo fascicolo documenti di formato diverso. Ad esempio, un *rendering*, a differenza di un modello, può essere inserito nel fascicolo di progetto di una costruzione. Cambiano i materiali e i supporti, ma la sostanziale importanza strategica dell'identificazione univoca del documento e delle aggregazioni documentali permane»⁷.

Dalla constatazione di una situazione poco governabile, nella consapevolezza che la conservazione nel tempo della documentazione (non solo quella giuridicamente rilevante, ma quella sull'attività professionale vera e propria) è cruciale per il futuro

⁵ A. Bilotto, M. Guercio, *Problemi e prospettive*, cit. p. 420.

⁶ G. Bonfiglio Dosio, *Tipologie documentarie di uno studio di progettazione*, in «Archivi», XVII/2 (lug.-dic. 2022), pp. 97-105. La citazione è a p.100.

⁷ *Ibidem*, p. 104. A questo saggio si rinvia per ogni ulteriore informazione sul lavoro.

dell'attività di uno studio di progettazione, è scaturito il ricorso agli archivisti per affrontare il tema. Già nel 2016, Kristine Fallon, architetta e pioniera nell'applicazione di IT nella progettazione, ne «Il giornale dell'architettura» del 28 giugno 2016, scriveva: «se lo studio non è attento al proprio archivio digitale, sarà poi difficile da parte di chiunque poterlo decifrare. Dalla nostra ricerca risulta che gli studi più grandi hanno maggiore capacità di organizzazione, anche per la necessità di garantire una migliore condivisione interna. Al contrario, gli studi più giovani si sono mostrati meno disciplinati a riguardo. Tendono ad usare qualsiasi tipo di software, anche interessante, però spesso mancano delle norme di base della gestione»⁸.

3. Conclusioni e auspici: archivisti nella nuvola

«...le potenzialità dell'informatica applicata all'archivistica sono l'unica via possibile per la conservazione della memoria digitale»⁹.

Questo implica una forte collaborazione, nel rispetto delle specifiche competenze professionali, per quanto proficuamente contaminate, evitando il rischio di dissoluzione delle abilità e professionalità nel mare della multidisciplinarietà, segnalato da Giovanni Michetti nel commentare la serie di norme ISO 30300 sulla gestione documentale¹⁰.

Del resto archivisti e informatici dedicano da tempo attenzione al tema dell'incontro fra le loro professionalità, qualche volta anche con una certa vivacità di approccio, e sul terreno della formazione esiste una consolidata tradizione per gli archivisti di acquisizione delle competenze necessarie per condividere con gli informatici i linguaggi necessari al dialogo. Prova ne sia che, finalmente, dopo che già le Università e le associazioni professionali come l'ANAI avevano messo al centro della loro attività di formazione il tema, nello scorso anno è stato varato il nuovo regolamento delle scuole di archivistica istituite presso gli Archivi di Stato che prevede uno specifico percorso per gli archivisti chiamati ad affrontare la conservazione della documentazione statale (e non solo) contemporanea.

«L'archivista non lavora più negli scantinati: è salito ai piani alti, disegna modelli e strategie documentali, coordina flussi, coadiuva i processi decisionali. In breve, governa una componente fondamentale del sistema informativo dell'ente. Talora sale anche più in alto, sul *cloud*, dove è chiamato a far interagire diversi *repository* secondo precisi modelli e *policy* documentarie»¹¹.

⁸ <https://ilgiornaledellarchitettura.com/2016/06/28/archivi-digitali-degli-architetti-ci-vuole-organizzazione/>.

⁹ A. Bilotto, M. Guercio, *Problemi e prospettive*, cit. p. 420.

¹⁰ G. Michetti, Giovanni Michetti, *Un approccio manageriale ai sistemi di gestione documentale: la serie ISO 30300*, in «Archivi & Cultura». *Archivi informatici. Problemi aperti nelle esperienze attuali e nelle prospettive future*, a cura di P. Carucci e M.L. Lombardo, a. 46-47 (2013-2014), pp. 99-120.

¹¹ G. Michetti, *Fra mito e realtà: la figura professionale dell'archivista*, in «Unione & Certificazione» 9 (2014), p. 13.

ESISTERÀ UNA GESTIONE DOCUMENTALE NEL 2026?

Andrea Piccoli

Abstract: Alla luce della trasformazione digitale della gestione dei procedimenti e attività amministrative ha ancora senso parlare di gestione documentale e di protocollo informatico? L'articolo propone una lettura d'insieme, senza entrare nei singoli dettagli degli argomenti toccati, al fine di porre in luce la differenza tra gestione documentale e gestione delle informazioni e gli impatti di tali riflessioni sui temi di conservazione digitale.

Considering the digital transformation of the management of process and administrative activities, does it still make sense to talk about document management and IT protocol? The article proposes an overall reading, without going into the individual details of the topics touched upon, in order to highlight the difference between document management and information management and the impacts of these reflections on digital preservation issues.

About European PNRR and the digital transformation of the management of process and administrative activities, we reflect on does it still make sense to talk about document management and public document electronic registration? The article proposes an overall reading, without going into the individual details of the topics touched upon, in order to highlight the difference between document management and information management and the impacts of these reflections on digital preservation issues.

Parole chiave: gestione documentale, protocollo informatico, PNRR, conservazione digitale

Sommario: 1. Introduzione – 2. Dal documento all'informazione – 3. eIDAS, mercato digitale unico europeo – 4. L'ecosistema digitale nazionale – 5. La gestione delle informazioni – 6. La conservazione delle informazioni – 7. Conclusioni

1. Introduzione

Perché aprire un articolo con una domanda? Ci sono un paio di motivazioni sottostanti alla domanda posta. La prima è perché dopo diversi anni in cui la digitalizzazione dei procedimenti e delle attività amministrative è proceduta con una tortuosa strada evolutiva, sia dal punto di vista normativo che tecnologico, spesso limitata dalla risorse messe a disposizione o peggio con la chimera della invarianza di bilancio, si osserva che l'attuazione del Piano Triennale per l'informatica della Pubblica

Amministrazione (2021 – 2023) e della Strategia PA 2026 supportata dalla spinta economica del Piano Nazionale Resilienza e Ripartenza (PNRR), e dagli obiettivi da perseguire di entrambi questi strumenti, sta portando una accelerazione nel cambiamento delle modalità di gestione dei procedimenti e attività amministrative. La seconda è che in questo cambiamento veloce e cadenzato dalle scadenze degli obiettivi e quindi degli avvisi delle diverse misure, e che prevede l'adozione di piattaforme e strumenti digitali nuovi, non si vogliono perdere di vista i presupposti di liceità dei procedimenti e delle attività amministrative e i principi dei diritti di cittadinanza digitale previsti dal Codice dell'Amministrazione Digitale. Infine, ci si chiede se proprio il Codice dell'Amministrazione Digitale e delle Linee Guida conseguenti, così come le norme del Testo Unico sulla Documentazione Amministrativa aggiornato con le modifiche apportate, da ultimo, dal D.L. 31 maggio 2021, n. 77, convertito, con modificazioni, dalla L. 29 luglio 2021, n. 108 che comprendono quelle del Protocollo Informatico del DPR 445 del 2000; non abbiano bisogno di una profonda revisione o riscrittura in logica digitale.

2. Dal documento all'informazione

La nostra cultura amministrativa, legata alla rappresentazione di atti e fatti giuridicamente rilevanti, è legata al documento. Con l'avvento delle tecnologie dell'informatica e telecomunicazioni si è poi passati ad introdurre il documento informatico, inteso come la rappresentazione digitale, nativamente digitale o frutto della digitalizzazione di una copia originaria di un documento analogico. E su questa dualità di documento informatico e di documento analogico si è poi sviluppata l'attuale normativa dedicata a descrivere le modalità di equivalenza di azioni quali la sottoscrizione (firma), la marcatura temporale, i sigilli e bolli e le modalità di creazione e gestione di copie conformi e di passaggi tra analogico e digitale e viceversa. L'archivistica, e in generale l'attenzione alla formazione, gestione e conservazione degli archivi documentali (correnti e storici, analogici e digitali) ha consentito di riconoscere il ruolo centrale degli strumenti di organizzazione dei documenti, a prescindere dal supporto, al fine di gestire componenti vitali della trasformazione digitale, tra cui il valore legale e l'efficacia probatoria dei documenti. Sul piano giuridico e notarile ci si limita a ricordare che senza le evidenze documentali, eventualmente repertorate e di fede pubblica, conservate, non esiste un procedimento amministrativo lecito.

Al contempo le tecnologie dell'informazione hanno introdotto nella nostra esperienza quotidiana soluzioni e piattaforme digitali di cui abbiamo completa esperienza e fiducia nei loro effetti. Un esempio in cui questa trasformazione digitale si è compiuta è quella legata alle banche online, o modelli ibridi tra banche fisiche e online: i nostri conti correnti sono digitali e le transazioni economiche avvengono su canali esclusivamente digitali e le cui evidenze ci sono trasmesse digitalmente. Qualche volta abbiamo bisogno del documento, del PDF per essere concreti nell'esemplifica-

zione, della copia contabile del bonifico appena fatto o dell'estratto conto periodico delle transazioni economiche effettuate con la carta di credito, ma si tratta di copie di informazioni digitali, trascritte su un documento informatico per renderle leggibili e interpretabili da noi, umani.

Le informazioni sono spesso riferite ad eventi che portano effetti di trasformazione dello stato iniziale. Ad esempio, un bonifico è un evento di transazione economica tra due soggetti che porta il saldo contabile del mittente a essere diminuito del medesimo importo economico accreditato sul saldo contabile del destinatario. Di questa elementare esemplificazione si vogliono richiamare due importanti concetti: il primo è che l'evento, la transazione economica, avviene solo e soltanto quando il trasferimento ha successo; il secondo è che l'esecuzione dell'evento richiede la interoperabilità digitale tra la soluzione della banca mittente e quella destinataria.

Si può quindi affermare che l'informazione sull'evento di transazione deve poter essere resa leggibile dall'utente umano; integra e interoperabile nel suo contenuto digitale, certa nella sua fonte e destinazione, conservata per il tempo da parte degli interessati per il necessario dei suoi effetti.

L'interoperabilità delle informazioni si può realizzare solo quando il formato di rappresentazione delle informazioni è interpretabile in modo informatico ed è condiviso nell'attribuzione di significato. Nel linguaggio tecnico si parla di schemi condivisi e di formati quali xml (eXchange Markup Language) o json (JavaScript Object Notation). Ma a parte gli aspetti tecnici di definizione di interfacce (API) e schemi comuni (XSD), il tema fondamentale è il vocabolario comune e condiviso, ovvero il significato funzionale che si attribuisce a ogni componente dell'informazione.

Le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici hanno rappresentato uno sforzo di apertura normativa verso la gestione delle informazioni. L'introduzione di schemi di metadattazione ricchi e standardizzati sia per i documenti informatici che per le loro aggregazioni; in quest'ultimo ambito con particolare attenzione ai sistemi di classificazione e ai fascicoli, che assicurano la completezza e la coerenza delle informazioni e dei documenti riferiti alla gestione dei procedimenti e delle attività amministrative. Al contempo ha rinnovato le indicazioni per la realizzazione dell'interoperabilità di protocollo.

Il passaggio ulteriore quindi necessario per il pieno sviluppo di una gestione documentale informatica, non solo sul piano tecnico e normativo, ma anche quello culturale amministrativo, è quello di abbandonare la visione del documento informatico come rappresentazione digitale di atti e fatti giuridicamente rilevanti esclusivamente associata a una sua rappresentazione e forma leggibile, per esempio alla sua restituzione in PDF e passare invece quanto più possibile alla rappresentazione nativa digitale delle informazioni e delle transazioni che la riguardano, supportando la leggibilità umana di tali informazioni e applicando opportuni fogli di stile. Del resto, l'introduzione della fatturazione elettronica ormai condivisa anche a livello europeo, associata anche alle informazioni sulle transazioni economiche legate a tali flussi, dovrebbe averci abituato a considerare l'originale informativo non solo la fattura in formato xml firmata digitalmente, ma anche le informazioni granulari e strutturate degli avvenuti pagamenti.

3. eIDAS, mercato digitale unico europeo

Certamente si può affermare che l'attuale evoluzione della digitalizzazione dei procedimenti e attività amministrative sia guidata anche dalla necessaria convergenza normativa e operativa italiana verso il regolamento europeo eIDAS, che fornisce una base normativa per le interazioni elettroniche fra cittadini, imprese e pubbliche amministrazioni incrementando la sicurezza e l'efficacia dei servizi online e transazioni e-business nell'Unione Europea.

Senza volersi dilungare ad una analisi degli articolati contenuti del regolamento europeo, al fine di contestualizzare quanto sta' avvenendo e avverrà nella realizzazione dell'ecosistema digitale nazionale, si vogliono richiamare alcuni servizi e componenti di base.

Il primo riguarda l'identità digitale dei cittadini europei che prevede l'associazione a credenziali forti (due fattori di autenticazione) ad un dispositivo (*wallet*) di possesso del cittadino. Nell'architettura tecnica è previsto un sistema federato di erogatori di identità (*trusted provider*) che mutuamente riconoscono come valide le identità emesse e gestite e realizzano un protocollo unico di autenticazione per i servizi che vogliono utilizzare l'identità digitale eIDAS. Sicuramente la carta d'identità elettronica (CIE) con la app CIEID e il connettore previsto per eIDAS sono già in linea con questa evoluzione.

Dal punto di vista delle tematiche di sottoscrizione digitale, firme elettroniche, marche temporali e sigilli, l'ampia normativa italiana è già adeguata a quanto previsto dall'eIDAS, anzi al limite è sovrabbondante nelle tipologie di firma previste.

Sul tema degli erogatori di servizi fiduciari di recapito elettronico emerge qualche esigenza di adeguamento normativo che porterà l'attuale posta elettronica certificata (PEC) a divenire un servizio di recapito fiduciario inteso come un *registered electronic email* (REM). L'evoluzione della PEC a servizio qualificato risiede proprio nel meccanismo di garanzia dell'autenticazione e identificazione di mittente e destinatario che passa attraverso la registrazione dell'utenza presso un service provider e nella individuazione della utenza identificata: il processo di registrazione prevede che il titolare dell'utenza venga "identificato" prima di utilizzare il servizio. Ciò garantirà la piena interoperabilità delle caselle di posta certificate e qualificate, con possibilità di scambio di documenti e atti a pieno valore legale attestandone data di trasmissione e ricezione. In modo analogo anche l'interoperabilità di protocollo informatico inizialmente orientata all'utilizzo della PEC, ed estesa all'uso di appositi servizi applicativi web nelle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici dovrà adeguarsi alla realizzazione dell'*e-Delivery* europeo, disegnato per le amministrazioni pubbliche con cui le stesse possono scambiare dati e documenti elettronici con altre amministrazioni pubbliche, imprese e cittadini, in modo interoperabile, sicuro, affidabile e fidato. Questo sistema è strutturato come una rete di nodi per le comunicazioni digitali, basato su un modello distribuito dove ogni partecipante diventa un nodo utilizzando protocolli di trasporto e politiche di sicurezza standard.

Infine, eIDAS introduce i servizi fiduciari qualificati di conservazione di firme; sigilli o certificati elettronici a supporto degli altri servizi previsti. E' chiaro che rispetto alla visione dei servizi di conservazione previsti attualmente dalla norma italiana, che hanno lo scopo di garantire nel tempo l'integrità, validità e disponibilità dei documenti conservati, la focalizzazione del regolamento eIDAS sulla conservazione delle firme appare come una sottolineatura agli aspetti di gestione della validità e affidabilità nel tempo dei documenti informatici con firme digitali, essendoci ovviamente uno scontato legame tra la firma digitale e il contenuto sottoscritto.

Lo standard ETSI 119 511 sviluppa i requisiti delle politiche generali per i prestatori di servizi fiduciari ed è relativo ai requisiti di sicurezza e alle politiche organizzative in materia di conservazione di lungo periodo delle sottoscrizioni digitali e altri dati generali come dati sottoscritti o non sottoscritti. Lo standard indirizza due scenari: la conservazione per lunghi periodi di tempo, con l'uso di tecniche di firma digitale, la capacità di convalidare una firma digitale, di mantenere nel tempo il suo stato di validità e di ottenere una prova dell'esistenza dei dati firmati associati così come erano al momento della presentazione al servizio di conservazione, anche se successivamente la chiave di firma viene compromessa, il certificato scade o gli attacchi crittografici diventano attuabili rispetto all'algoritmo della firma o nell'algoritmo di hash utilizzato nella firma in esame; la fornitura di una prova dell'esistenza di oggetti digitali, indipendentemente dal fatto che siano firmati o meno, utilizzando tecniche di firma digitale eventualmente con marca temporale e le registrazioni di prove. E' chiaro che rispetto alla finalità di conservare nel tempo le informazioni relative ai procedimenti e attività amministrative che hanno avuto effetto giuridico e che possono essere rilevanti da un punto di vista storico archivistico l'attuale normativa italiana sui servizi di conservazione ha una più ampia attenzione alla conservazione dei contenuti e della loro meta datazione.

4. L'ecosistema digitale nazionale

Come presentato in apertura le diverse progettualità legate agli obiettivi del PNRR stanno andando a definire e rendere concrete alcune piattaforme digitali a corredo della digitalizzazione del rapporto tra cittadini e imprese con la pubblica amministrazione, e di riflesso tra le stesse pubbliche amministrazioni.

Il tema delle identità digitali, SPID e CIE, con particolare attenzione alla seconda che prevede anche l'implementazione del connettore eIDAS europeo, permette in tutti i casi in cui è necessario di avere certezza, nei livelli richiesti, della identità dei soggetti coinvolti. Lato pubbliche amministrazioni l'introduzione del sigillo elettronico quale strumento per verificare la paternità delle informazioni comunicate permette di rendere certa l'identità dell'amministrazione che comunica.

Tali strumenti di identità digitale permettono di allargare ed estendere l'utilizzo delle firme elettroniche qualificate, permettendo al cittadino di sottoscrivere digitalmente del-

le informazioni ad esempio fornite per mezzo della compilazione di modulistica online. L'AppIO, che ha trovato una iniziale diffusione, purtroppo, nel periodo pandemico e legata alla attribuzione di qualche bonus economico; si presenta come lo strumento digitale in cui il cittadino può non solo ricevere comunicazioni e avvisi dalle pubbliche amministrazioni ma anche fruire in modo nativo digitale, come ad esempio la richiesta di documenti o l'invio di modulistica per richiedere benefici e servizi, ed eventualmente procedere al pagamento di alcuni doveri se previsti per mezzo di PagoPA. L'integrazione di tali servizi, vista dalla pubblica amministrazione aderente comporta già una serie di problematiche da indirizzare all'interno della gestione documentale e del protocollo informatico.

Ad esempio, ci si aspetta che il cittadino, utilizzando la propria AppIO, autenticatosi, possa inserire una richiesta di accesso ad un beneficio, come ad esempio l'iscrizione al servizio della mensa scolastica. Lato pubblica amministrazione tale richiesta rappresenta un'informazione digitale, sottoscritta con firma elettronica avanzata che deve essere protocollata ed avviare il procedimento amministrativo che si concluderà con la comunicazione da parte dell'amministrazione dell'accoglimento della richiesta e l'invio della richiesta di pagamento della retta. Al contempo la gestione di tale richiesta potrebbe scatenare una transazione nel sistema di gestione dei servizi scolastici. Ora necessariamente si deve pensare che l'informazione generata dal cittadino richiedente non è necessariamente un PDF, né che lo debba diventare all'interno del protocollo informatico e della gestione documentale, almeno fino a quando non sia necessario crearne una copia leggibile per l'umano. Anzi se nativamente nella comunicazione tra AppIO e la gestione documentale andasse persa l'informazione digitale nativa, a favore della sua conversione in PDF prima della protocollazione, si perderebbe l'opportunità di sviluppare in modo tecnicamente agevole la comunicazione con il gestionale verticale.

Anche i servizi web presenti nei siti delle amministrazioni, grazie al profuso impegno di Design Italia e agli ampi finanziamenti previsti dagli avvisi della "Esperienza del Cittadino", costituiscono al contempo uno sforzo di standardizzazione della modalità con cui il cittadino si troverà ad operare nei diversi servizi web offerti dalle amministrazioni a vantaggio della più semplice fruizione, ma anche e soprattutto una linea guida di standardizzazione delle informazioni digitali che il sito web scambia nel dialogo con il sistema di gestione delle informazioni, sia quello del protocollo informatico che degli altri verticali specifici, dell'ente per erogare il servizio al cittadino all'interno del procedimento o attività amministrativa istaurata da quest'ultimo. Le considerazioni sugli impatti della gestione documentale non sono dissimili da quelli appena condivisi per la AppIO, cambiando lo strumento di iterazione ma non lo scenario funzionale.

L'altra piattaforma che entra a stretto contatto con la digitalizzazione delle attività amministrative è la Piattaforma Notifiche Digitali (PND) che permette alle pubbliche amministrazioni di inviare le notifiche e provvedimenti amministrativi in forma nativa digitale, delegando alla piattaforma la gestione delle modalità di notifica, collegate al domicilio digitale eletto nella piattaforma da ogni cittadino, e di ricevere evi-

denza dell'avvenuta consegna dell'avviso e dell'atto notificato stesso. La piattaforma PND integra eventualmente la possibilità da parte del cittadino di procedere al pagamento del dovuto attraverso PagoPA. Una prima sottolineatura su questa piattaforma merita in fatto che essa svolge anche il ruolo, lato cittadini ed imprese di elezione del proprio domicilio digitale potendo optare per un indirizzo di posta elettronica certificata, la propria AppIO o l'indirizzo di residenza fisico. Da un punto di vista degli impatti sulla gestione documentale e protocollo informatico, il primo è strettamente legato alla gestione dei destinatari degli atti da notificare, ove solo una completa integrazione delle anagrafiche dei cittadini, rappresentanti di imprese, tutori o professionisti comprensiva dei loro domicili digitali permette un corretto indirizzamento della notifica e meta datazione del protocollo in uscita. Mentre in questo caso con molta probabilità il documento notificato sarà un PDF firmato digitalmente, un impatto importante nella gestione della unità documentaria del protocollo in uscita è l'associazione delle diverse ricevute informatiche che saranno rese disponibili dalla integrazione con la piattaforma di notifica in corrispondenza dei diversi eventi che hanno rilevanza giuridica, come la consegna dell'avviso o l'effettivo recapito della notifica e l'eventuale evento di avvenuta riscossione del dovuto. Queste ultime sono informazioni digitali, non associate ad una loro rappresentazione testuale PDF, ma di grande importanza giuridica sul procedimento amministrativo in corso.

La Piattaforma Digitale Nazionale Dati apre la strada della interoperabilità dei dati amministrativi necessari alle pubbliche amministrazioni per dialogare in modo nativo digitale, rendendo possibile il diritto di cittadinanza digitale di fornire i propri dati una sola volta alla pubblica amministrazione, secondo il concetto del "*once only*". Il modello realizzativo della piattaforma è pensato in modo da garantire alle amministrazioni pubbliche aderenti di organizzare le integrazioni attorno ai loro processi e non viceversa. Da un punto di vista degli impatti nella gestione documentale si sottolineano due aspetti: il primo è relativo all'opportunità di integrazione delle anagrafiche non solo dei soggetti in quanto tali, ma delle loro aggregazioni legate ad aspetti di organizzazione amministrativa dei procedimenti, per esempio l'elenco dei professionisti di un certo ordine, oppure della popolazione che in una certa zona geografica gode di particolari benefici legati alla propria posizione personale, oppure l'elenco delle attività produttive o dei cantieri per gli procedimenti di sanità pubblica.

5. La gestione delle informazioni

Alla luce di quanto fin qui analizzato e condiviso, appare più chiaro il senso della domanda posta all'inizio di questa riflessione. La risposta è che per supportare e accompagnare la transizione al digitale della formazione e gestione delle informazioni digitali rilevanti per i procedimenti e attività amministrative è necessario ripensare l'architettura, le modalità operative e la normativa a supporto della gestione docu-

mentale, ma non di perderne i vantaggi.

Da un punto di vista normativo sarebbe auspicabile lasciare al Codice dell'Amministrazione Digitale la definizione dei diritti di cittadinanza digitale e dei principi guida in modo da averne una versione stabile nel tempo e non influenzata dall'evoluzione tecnologica, al contempo indirizzare la necessità di standard tecnici e di vocabolari e schemi comuni per la descrizione delle informazioni digitali giuridicamente rilevanti, degli eventi e delle metadazioni collegate. Anche il Testo Unico sulla Documentazione Amministrativa dovrebbe essere ridefinito riconoscendo la rilevanza delle informazioni di cui il documento è costituito e cui fa riferimento nei processi di gestione amministrativa.

Da un punto di vista realizzativo la gestione delle informazioni digitali associate alle attività amministrative necessita di soluzioni pensate per dialogare ed essere interoperabili sia all'interno dell'amministrazione con le altre soluzioni gestionali verticali, sia all'esterno con l'ecosistema digitale nazionale. In questo dialogo si devono gestire non solo le informazioni amministrative che si vanno formando e comunicando, all'interno dei fascicoli ma anche tutti quegli eventi giuridicamente rilevanti che tracciano il progredire del procedimento.

La gestione dei documenti e delle informazioni è in sostanza un supporto aperto alla gestione dei procedimenti e delle attività amministrative della PA finalizzato a definire passi transazionali e procedurali, individuando le responsabilità connesse e le unità informative, documentarie e archivistiche che si vanno formando e gestendo e dall'altra parte un gestore di eventi e delle informazioni connesse, scambiati in modo interoperabile nell'ambito dell'ecosistema digitale interno ed esterno all'amministrazione.

Per garantire la qualità delle soluzioni e servizi, magari in logica cloud e *Software as a Service* (SaaS), sarebbe auspicabile riprendere il lavoro di stesura di una checklist di valutazione della qualità delle soluzioni di gestione delle informazioni e provvedere ad una loro qualificazione, estendendo quanto già introdotto per gli aspetti di sicurezza e protezione delle informazioni.

6. La conservazione delle informazioni

Come ormai al lettore apparirà chiaro dalla lettura del contesto della evoluzione della digitalizzazione dei procedimenti e attività amministrative anche il tema della conservazione dei documenti necessita di essere ripensata in una conservazione delle informazioni digitali.

La prima considerazione è che le informazioni digitali relative agli eventi associati alla vita amministrativa delle unità informative sono molteplici, articolate, importanti per descrivere il contenuto e la sua efficacia giuridica e sono accompagnate da una ricca meta datazione che ne descrive il contesto amministrativo. È quindi necessario porre attenzione alla descrizione delle unità informative (unità documentali, qui

rinominate per evidenziarne l'evoluzione nel loro contenuto informativo) nelle loro componenti e fornirne una consistente rappresentazione nel formato di interoperabilità UNI SInCRO. A seguire anche le unità amministrative (unità archivistiche, qui rinominate per sottolinearne l'aspetto di rappresentazione di un procedimento o attività amministrativa) vanno descritte nell'insieme delle unità informative, non tutte necessariamente di tipo amministrativo, e meta datazione che descrivano l'intero procedimento o attività comprese le interazioni con le altre soluzioni e piattaforme che hanno portato effetti giuridici rilevanti; una struttura complessa e ricca da comunque portare in una consistente rappresentazione nel formato di interoperabilità per la conservazione.

La seconda considerazione nasce dall'osservazione dei volumi ed eterogeneità di queste informazioni messe in relazione con il tema della conservazione di lungo periodo e la necessità di rendere fruibili e sedimentate le informazioni rilevanti. Se si legge la conservazione come lo strumento necessario non solo a garantire l'integrità delle informazioni nel tempo ma anche la loro fruizione da parte della comunità di riferimento per avere una rappresentazione degli atti e fatti giuridicamente rilevanti del procedimento amministrativo conservato, appare chiaro che data la ricchezza (volumi) ed eterogeneità delle informazioni conservate sia necessario pensare ad una estensione del concetto di riversamento, più un consolidamento informativo, che raccolga in un formato idoneo alla conservazione di lungo periodo un estratto delle informazioni giuridicamente rilevanti da mantenere nella conservazione.

Collegata a questa considerazione vi è anche quella relativa alla necessità di distinguere, forse anche a livello normativo, la conservazione di breve periodo utilizzata per garantire la l'integrità e disponibilità delle informazioni conservate per i tempi necessari dalla conservazione di lungo periodo che tiene conto più dell'esigenza di conservare nel tempo le informazioni di interesse giuridico e storico degli atti amministrativi. Vero è il concetto dello scarto, però ancora poco applicato nei servizi di conservazione digitale e che dal punto di vista normativo ha bisogno di essere rivisto nell'ottica della conservazione delle informazioni.

7. Conclusione

Di sicuro uno dei fattori che può spingere l'adeguamento delle consuetudini amministrative è l'evoluzione delle soluzioni e dei servizi cloud orientati alla gestione documentale, anzi alla gestione dei documenti e delle informazioni e alla loro conservazione.

Il riuso delle soluzioni dovrebbe rendere evidente, selezionare e favorire le soluzioni che hanno caratteristiche di qualità funzionale, sicurezza e protezione delle informazioni idonee ad essere adottate. Soluzioni che dovrebbero avere un processo di qualificazione idoneo per portarle a garantire i requisiti necessari alla loro adozione come strumenti guida della trasformazione digitale.

Al contempo le soluzioni cloud presenti nel Marketplace non hanno solo bisogno di elevati livelli di sicurezza e protezione delle informazioni, guidati dai recenti nuovi requisiti della Agenzia per la Cybersecurity Nazionale, ma anche di una qualificazione di qualità funzionale mirata ad essere strumenti guida della trasformazione digitale nelle amministrazioni che le adottano.

GLI ARCHIVI DIGITALI E L'ART. 2086 C.C.: UNA RISPOSTA AL PRINCIPIO DI ADEGUATEZZA DELLA STRUTTURA

Giuseppe Vitrani

Abstract: L'articolo analizza il quadro generale normativo relativo agli obblighi di conservazione dei documenti digitali e di nomina del responsabile della conservazione da parte dei soggetti privati. Vengono inoltre analizzate le interazioni con la normativa codicistica e in particolare le relazioni esistenti con il principio di adeguatezza della struttura posto dall'art. 2086 c.c.

The article analyzes the general regulatory framework relating to the obligations of preservation of digital documents and the appointment of the preservation manager by private subjects. It also conducted an analysis about the existing relationships with the principle of adequacy of the structure established by art. 2086 of the civil code.

Parole chiave: archivio digitale, responsabile della conservazione, adeguatezza della struttura, Codice civile

Sommario: 1. Il quadro normativo generale – 2. Le previsioni delle linee guida – 3. Le interazioni con il Codice civile – 4. Il ruolo fondamentale dell'archivio digitale e del responsabile della conservazione.

1. Il quadro normativo generale

L'entrata in vigore delle Linee Guida AgID sulla formazione gestione e conservazione del documento informatico ha portato con sé l'interrogativo circa l'obbligo per i soggetti privati di nominare formalmente la figura del responsabile della conservazione.

A far da sfondo al tema c'è evidentemente l'art. 44, comma 1-ter, CAD ai sensi del quale "in tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida".

Se si pensa al mondo privato, in particolare al contesto aziendale, gli esempi concreti in cui effettivamente sussiste quest'obbligo non sono pochi; basti pensare alle scritture contabili tenute in modalità informatica ai sensi dell'art. 2215 bis c.c., che devono essere conservate per dieci anni dalla data dell'ultima registrazione. Inoltre, per uguale tempo, devono conservarsi anche fatture e corrispondenza aziendale (art. 2220 c.c.).

Altri esempi possono trarsi anche dal mondo delle professioni: si pensi all'obbligo decennale di conservare i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo; laddove tali dati siano raccolti mediante documenti informatici si configura evidentemente la necessità che la loro conservazione rispetti la normativa in commento. Sul punto si può peraltro affermare che la novella del Codice dell'amministrazione del 2020 ha sopito ogni dubbio: le modalità di conservazione sono quelle dettate dalle suddette Linee Guida e che sostanzialmente si possono tradurre nell'implementazione di un archivio digitale rispettoso dello standard ISO 14721:2012 (OAIS) integrato con la norma UNI 11386, ora nella versione 2020 (la cui tenuta può essere naturalmente affidata in outsourcing a terzi soggetti qualificati). Nessun dubbio, pertanto, può esserci circa la necessità di adottare un effettivo processo di conservazione a norma anche in ambito aziendale (e professionale), che dovrà essere necessariamente preceduto dal censimento dei documenti che dovranno popolare l'archivio digitale e dalla ricognizione dei metadati necessari per poter avviare effettivamente ed in maniera proficua l'iter di archiviazione.

2. Le previsioni delle linee guida

Il dubbio, invece, è se per lo svolgimento di tale attività sia obbligatoria la nomina di un responsabile o se tale passaggio formale possa essere omesso. Per provare a risolvere la questione è fondamentale leggere le Linee Guida, le quali, nella sezione dedicata alla conservazione (paragrafo 4.5), prevedono che:

“Nella Pubblica Amministrazione, il responsabile della conservazione:

- è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
- è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
- può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione”.

Per fornire una risposta è sufficiente interpretare cosa si intenda per “soggetti diversi dalla Pubblica Amministrazione”, come da locuzione riportata al secondo comma della norma in esame.

Le alternative ipotizzabili sono invero due:

- tutti i soggetti possibili e immaginabili, quindi anche i privati;
- oppure i soggetti, diversi dalle pubbliche amministrazioni, di cui all'art. 2, comma 2, lett. b) e c) del CAD (gestori di servizi pubblici, società soggette a controllo pubblico ecc.).

L'interpretazione, che va condotta alla luce di quanto prevede la norma primaria, non è pacifica; tuttavia la prima opzione appare preferibile soprattutto alla luce del disposto dell'art. 44, comma 1 ter CAD che obbliga i privati ad adottare un archivio digitale che sia conforme alle Linee Guida; invero, appare una conseguenza logica e coerente la previsione secondo cui anche tali soggetti debbano nominare un soggetto che assuma su di sé la responsabilità di monitorare il corretto funzionamento di questo delicato processo documentale.

3. Le interazioni con il Codice civile

L'analisi in diritto non può però fermarsi all'esame del solo combinato disposto delle norme più prettamente dedicate al digitale ma deve prendere in considerazione anche quanto prevede il Codice civile. È infatti opportuno ricordare che, ai sensi del secondo comma dell'art. 2086 c.c., "l'imprenditore, che operi in forma societaria o collettiva, ha il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale, nonché di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuità aziendale".

La norma fonda il cosiddetto principio dell'adeguatezza della struttura che non può certamente essere obliterato nel momento in cui si intraprende un passaggio critico come quello dell'assoggettamento a conservazione di documenti di importanza rilevante per l'azienda. E da questo punto di vista non può non considerarsi come l'adozione di un archivio digitale rispettoso della normativa sopra esaminata e la nomina di un soggetto che possa fungere da supervisore di tutte le operazioni legate all'avvio e alla gestione dello stesso non possa che essere indice del rispetto del suddetto principio.

Operando in questo modo l'azienda dimostrerebbe l'adeguatezza della propria struttura amministrativa, soprattutto nell'ambito della gestione di quei documenti che hanno terminato la fase di gestione corrente e che perciò devono essere indirizzati in un ambiente diverso da quello dell'ordinario sistema di gestione.

La tesi appare ancora più valida laddove si consideri che spesso detti documenti contengono dati personali che devono essere adeguatamente protetti; in tal senso l'archivio digitale appare senz'altro il luogo corretto, non fosse altro perché i soggetti conservatori sono di fatto obbligati a conformarsi ai rigidi standard imposti dall'AgID anche in tema di compliance con il regolamento europeo n. 679 del 2016.

4. Il ruolo fondamentale dell'archivio digitale e del responsabile della conservazione

L'adozione dell'archivio digitale e la nomina del responsabile della conservazione appaiono dunque fondamentali in ambito aziendale; si pensi infatti ad esempio alle attività di revisione contabile effettuate dal collegio sindacale (o dagli altri soggetti preposti all'attività in esame) o, ancor di più, alle attività di verifica condotte dalle autorità pubbliche (es. Agenzia delle Entrate o Guardia di Finanza). Anche in tal caso la presenza di un punto di riferimento dotato di competenze archivistiche sarà opportuna in quanto un'attività di esibizione di documentazione in grado di comprovare la corretta conservazione dovrà passare attraverso la generazione di un pacchetto di distribuzione; certamente una figura dotata di specifiche cognizioni potrà essere d'aiuto anche in questo frangente.

Sul punto è peraltro opportuno valutare la portata della novella di cui al decreto legge 73 del 2022, che ha aggiunto il comma 4-quater all'art. 7 del d.l. 357 del 1994; la norma dispone in particolare che “la tenuta e la conservazione di qualsiasi registro contabile con sistemi elettronici su qualsiasi supporto sono, in ogni caso, considerate regolari in difetto di trascrizione su supporti cartacei nei termini di legge o di conservazione sostitutiva digitale ai sensi del codice di cui al decreto legislativo 7 marzo 2005, n. 82, se in sede di accesso, ispezione o verifica gli stessi risultano aggiornati sui predetti sistemi elettronici e vengono stampati a seguito della richiesta avanzata dagli organi procedenti ed in loro presenza”.

Al di là delle inesattezze terminologiche (non si comprende l'utilizzo dell'aggettivo “sostitutiva”, ad esempio) la norma non appare idonea a scalfire il ragionamento condotto sino ad ora dal momento che codifica una strana condizione di regolarità di tenuta dei registri contabili che appare destinata ad operare in un caso specifico, ovvero quello dell'accesso, ispezione e verifica ma non si occupa della gestione ordinaria dei registri contabili.

Diverso scenario sarebbe quello ben più grave del default aziendale; in ipotesi del genere, il rispetto della normativa in tema di conservazione dei documenti aziendali sarebbe fondamentale per dimostrare la corretta tenuta delle scritture contabili, posto che il curatore non sarebbe vincolato dal suddetto art. 7, comma 4-quater, d.l. 357/1994 e legittimamente potrebbe pretendere l'esibizione di documenti digitali conservati a norma, trattandosi degli unici esemplari in grado di assicurare integrità e immodificabilità dei registri contabili.

Laddove l'azienda non fosse in grado di ottemperare non potrebbero escludersi conseguenze dirette sulle responsabilità penali degli amministratori, oltreché su quelle civili, stante che l'ipotetico curatore potrebbe decidere di perseguire con l'azione di responsabilità.

Un dato appare dunque inconfutabile: anche per l'azienda è imprescindibile conservare il digitale nel rispetto della normativa prevista dal codice dell'amministrazione digitale e dalle linee guida, sicché la presenza di un preposto/responsabile dotato di

competenza archiviste informatiche è certamente indice di adeguatezza della struttura organizzativa e amministrativa.

Da ultimo appare peraltro opportuno ricordare l'importanza dell'archivio digitale anche in sede probatoria in caso di contenzioso; con pregevole sentenza del 2019 la Corte di Cassazione ha infatti affermato che il valore della prova legale del supporto informatico è subordinato al rispetto delle regole tecniche di produzione e conservazione dello stesso; in difetto del rispetto di queste, l'idoneità del documento informativo a soddisfare il requisito della forma scritta ed il suo valore probatorio sono liberamente valutabili in giudizio (Cass. 11 febbraio '19, n. 3912).

STRATEGIE E BUONE PRATICHE PER LA SELEZIONE DEI DOCUMENTI INFORMATICI: SOTTOFASCICOLI, SFOLTIMENTO E CAMPIONATURA

Dimitri Brunetti

Abstract: Nel contesto della transizione al digitale della Pubblica Amministrazione e dell'informatizzazione della gestione documentale, il tema della selezione sta assumendo una considerevole importanza poiché siamo chiamati a sviluppare nuovi modelli e ad operare delle scelte in un ambiente che non padroneggiamo ancora del tutto. Scegliere cosa conservare e cosa lasciare è una decisione impegnativa e la redazione del Piano di selezione e conservazione è indispensabile. È però possibile andare oltre con la formazione dei sottofascicoli, con lo sfoltimento delle aggregazioni documentali e con la campionatura, tecniche che possono ridurre progressivamente la massa documentaria e che rendono più efficace la generazione dell'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto.

In the context of the transition to digital public administration and the computerisation of document management, the subject of selection is assuming considerable importance as we are called upon to develop new models and make choices in an environment that we do not yet fully master. Choosing what to keep and what to leave behind is a challenging decision and the drafting of the Selection and Preservation Plan is indispensable. However, it is possible to go further with the formation of sub-files, with the thinning of document aggregations and with sampling, techniques that can progressively reduce the mass of documents and that make the generation of the list of archiving packages containing documents destined for discarding more efficient.

Parole chiave: archivio digitale, documenti informatici, selezione, scarto, sottofascicoli, sfoltimento, campionatura

Sommario: 1. I sottofascicoli - 2. Lo sfoltimento - 3. La campionatura

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici approvate dall'Agenzia per l'Italia digitale propongono il termine «selezione» 16 volte e la parola «scarto» 31 volte. D'altra parte anche i decreti regolamentari del 2013 e 2014 e il DPR 445 del 2000 ponevano frequentemente l'attenzione sulle operazioni di selezione, e così fanno, in genere, tutte le norme e le disposizioni sulla gestione documentale. Però, non si tratta di un'attenzione inconsueta perché il tema

della selezione dei fascicoli d'archivio, ovvero l'operazione con cui li si suddivide fra quelli da conservare illimitatamente e quelli da custodire solo per un tempo definito, è sempre stato un argomento di riflessione fra gli archivisti ed è oggetto di discussioni che hanno portato all'elaborazione di modelli ed elenchi¹. È comunque fuor di dubbio che nel contesto della gestione digitale degli archivi contemporanei il tema abbia acquisito una rilevanza maggiore perché il problema della scelta si è fatto più delicato. Accantonata l'idea balzana che il documento digitale non occupa spazio e non costa nulla e che quindi si può tenere tutto senza problemi per sempre, si è rafforzata la convinzione che è essenziale ridurre progressivamente il numero delle aggregazioni documentali sia per diminuire i costi (e qui si potrebbe anche richiamare l'impronta ecologica degli archivi elettronici), sia per favorire la ricerca e il diritto d'accesso. Inoltre, se nella gestione analogica dei documenti si erano ormai consolidate regole, prassi e abilità che rendevano l'operazione della selezione abbastanza routinaria, nell'ambito digitale tali capacità vengono a mancare e tutto diventa più complesso. In ultimo, la selezione documentale elettronica ha modificato profondamente la prospettiva con la quale si è sempre guardato allo scarto: se con le carte il momento della scelta si collocava quasi esclusivamente nel versamento, cioè nel passaggio della documentazione dall'archivio di deposito all'archivio storico, ora la decisione dev'essere presa prima e viene anticipata fino al momento della formazione quando nel Piano di conservazione siamo chiamati ad indicare, a fianco delle voci di classificazione e delle indicazioni delle aggregazioni documentali previste al loro interno, il numero degli anni di tenuta dei materiali, anche in armonia con il Codice civile e la normativa di riferimento.

Oggi di selezione nel contesto digitale si parla tanto, anche se l'accento viene posto in modo improprio sullo scarto. Però, temo, nessuno realmente la mette in pratica. Un po' perché la documentazione elettronica correttamente archiviata è ancora molto recente, un po' perché se ne ha una gran paura. Eppure bisognerà iniziare e sarà indispensabile farlo bene, molto bene, perché lo scarto è necessario, ma e anche l'unica operazione archivistica senza ritorno. Una volta eliminato un documento, un fascicolo o una serie, anche se si tratta di materiali informatici con tutte le loro copie, non c'è alcuna possibilità di ripensarci e recuperare quello che è stato distrutto. Questo contributo non si propone di affrontare in senso ampio il tema della selezione e dello scarto dei documenti informatici e neppure analizzare la normativa o la bibliografia. Ci si vuole invece soffermare su pratiche particolari, tanto difficili da applicare quanto valide. Tecniche forse raffinate e complesse, ma che aiutano nel momento della scelta e che rendono molto più efficace l'operazione con cui si «gene-

¹ Per un primo approccio al tema si vedano: Gianni Penzo Doria, *Scarto di dati, selezione di documenti*, in «Atlanti», vol. 31 (2021), n. 2, pp. 131-151, <https://journal.almamater.si/index.php/Atlanti/issue/view/37>; Paola Carucci e Maria Guercio, *Manuale di archivistica*, Roma, Carocci, 2021² (in particolare: 13. *Lo scarto*, pp. 359-376; 16. *La conservazione dei documenti digitali*, pp. 459-482); *Lo scarto. Teoria, normativa e prassi*, a cura di Gilberto Zacchè, San Miniato, Archilab, 2002 (in particolare: Gianni Penzo Doria, *Massimario e prontuario: la selezione dei documenti dopo la riforma della pubblica amministrazione (1997-2001)*, pp. 57-94).

ra l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto» nel «rispetto dei termini temporali stabiliti dal piano di conservazione»².

Si tratta della formazione di sottofascicoli con i quali segmentare la documentazione di diverso valore, dello sfoltimento ovvero dell'estrazione ed eliminazione dei file inutili all'interno del fascicolo, della campionatura con cui si conserva solo una piccola parte dei fascicoli che costituiscono una serie. La particolarità di queste tecniche risiede in due elementi che coinvolgono il momento in cui vengono applicate e il soggetto che le realizza. La sotto-fascicolatura si fa nel corso dello svolgimento della pratica, quindi nella fase corrente, lo sfoltimento e la selezione dei campioni si realizzano al momento del trasferimento dall'archivio corrente all'archivio di deposito, quindi nel passaggio dal sistema di gestione documentale a quello di conservazione. E non è il responsabile della gestione documentale o l'archivista che attua queste operazioni, ma il responsabile del procedimento e quindi si tratta di attività distribuite, che coinvolgono un gran numero di persone, messe in pratica senza un reale controllo centrale e che quindi richiedono una comprensione ampia e distribuita delle pratiche conservative che si può raggiungere solo tramite frequenti momenti di formazione.

1. I sottofascicoli

Il Manuale di gestione deve fornire le istruzioni per la formazione delle aggregazioni documentarie e il Piano di conservazione deve indicare quali tipologie di serie e di fascicoli si formano in riferimento a ciascuna voce di titolario, quali documenti sono presenti al loro interno e le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto³. Il Piano di conservazione, che sovente assume la denominazione più articolata di «Piano di fascicolatura, selezione e conservazione», è uno strumento utile e complesso che svolge la sua azione in molti momenti del ciclo documentario: indica le modalità di formazione dei fascicoli nell'archivio corrente, consente l'identificazione e la protezione dei fascicoli di maggior valore, permette lo spostamento dei documenti fra diverse aree del sistema di conservazione, facilita la selezione e lo scarto dei materiali privi di importanza.

Il fascicolo è un'aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento⁴. Esso

² *Linee guida sulla formazione, gestione e conservazione dei documenti informatici, 4.11 Selezione e scarto dei documenti informatici, par. 3.*

³ *Linee guida sulla formazione, gestione e conservazione dei documenti informatici, 3.5 Manuale di gestione documentale, punti 4 e 5.*

⁴ *Linee guida sulla formazione, gestione e conservazione dei documenti informatici, Allegato 1 Glossario dei termini e degli acronimi, voce Fascicolo informatico.*

è costituito dai documenti relativi ad una determinata pratica, ma nel caso della formazione di fascicoli corrispondenti a procedimenti amministrativi complessi, o ad iniziative che danno origine ad una moltitudine di attività, magari coinvolgendo anche più unità organizzative ed eventualmente enti diversi, solitamente si procede a suddividere i fascicoli al loro interno in sottofascicoli, in modo da formare aggregazioni di documenti facilmente gestibili e riconducibili ad una determinata sequenza di attività⁵.

I sottofascicoli possono assolvere anche alla funzione di sedimentare la documentazione di differente valore, così da avvicinare quelli di maggiore importanza amministrativa e legale, i materiali raccolti come documentazione di supporto e i documenti di valore temporaneo oppure non strettamente associati al procedimento o affare. La suddivisione in fascicoli è lasciata alla discrezionalità del responsabile del procedimento⁶, che valuta caso per caso quando la documentazione assume particolari aspetti da richiederne la distinzione nel suo ambito, ma può anche essere indicata nel Piano di fascicolatura e conservazione, e in tal caso ne va precisata l'obbligatorietà o meno.

Le Linee guida AgID sui documenti informatici prevedono che a ciascun fascicolo venga associato il metadato con l'indicazione del tempo di conservazione⁷, ma nulla osta a che anche ai sottofascicoli vengano collegati specifici tempi di tenuta, che naturalmente non potranno essere più lunghi rispetto a quelli indicati per il fascicolo cui sono uniti. Quindi i sottofascicoli possono essere identificati anche con tempi di conservazione inferiori rispetto al loro fascicolo di appartenenza e pertanto i sottofascicoli potranno essere selezionati per lo scarto in modo autonomo, così da ridurre progressivamente la quantità dei documenti conservati e i relativi costi.

Ad esempio, un fascicolo riferito ad un procedimento contiene al suo interno documenti dal valore amministrativo, giuridico e culturale rilevante raccolti in un sottofascicolo a conservazione illimitata, poi documentazione contabile da conservare per dieci anni, infine materiali transitori di cui si prevede la conservazione per soli cinque anni. In questo modo il sistema di conservazione potrà includere nell'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto il sottofascicolo con i materiali transitori dopo soli cinque anni dalla chiusura del fascicolo e dalla sua ricezione definitiva da parte del medesimo sistema conservativo con generazione del rapporto di versamento relativo ai pacchetti contenenti i materiali in oggetto. Il fascicolo rimarrà nell'archivio digitale con i soli due sottofascicoli contenenti rispettivamente i documenti più importanti e la documentazione contabile

⁵ Stefano Pigliapoco, *Guida alla gestione informatica dei documenti*, Torre del Lago Puccini, Civita editoriale, 2020, p. 122.

⁶ Legge 7 agosto 1990, n. 241, artt. 5 e 6; D.Lgs. 7 marzo 2005, n. 82, art. 41.

⁷ *Linee guida sulla formazione, gestione e conservazione dei documenti informatici, Allegato 5 I metadati*, par. 4 *Metadati delle aggregazioni documentali informatiche*, p. 87 (*Definizione del metadato Tempo di conservazione*). Sebbene le Linee guida non facciano riferimento ai sottofascicoli e alle sottoserie, queste ripartizioni sono previste dal citato Allegato 5, p. 87 (*Definizione del metadato Identificativo dell'Aggregazione Primaria*).

fino a che, dopo altri cinque anni, anche questo secondo sottofascicolo verrà avviato allo scarto. In questo modo i costi di conservazione si riducono a mano a mano che la documentazione perde valore e il fascicolo destinato alla conservazione illimitata sarà formato dai soli documenti vitali.

2. Lo sfoltimento

Una volta conclusa la pratica e chiuso il fascicolo, prima del trasferimento dall'archivio corrente a quello di deposito, è buona abitudine sfoltire il fascicolo dei documenti dichiarati inutili⁸. Lo sfoltimento si realizza estraendo ed eliminando i documenti di carattere strumentale e transitorio utilizzati per espletare il procedimento, che hanno esaurito la loro funzione nel momento in cui è stato emesso il provvedimento finale, oppure quelli che non sono strettamente connessi al procedimento stesso. Documenti, quindi, che sicuramente non sono più utili per l'azione amministrativa, che non svolgono una funzione di testimonianza legale e che non acquisiranno alcun valore storico o culturale. Si tratta, ad esempio, di appunti, promemoria, minute, copie, normativa, moduli, documenti di carattere generale, materiali acquisiti come documentazione o come precedente, documenti interlocutori. In una prima fase del percorso di transizione al digitale questo genere di documenti non veniva ricompreso nella gestione dei procedimenti e non finiva nei fascicoli elettronici rimanendo invece su carta o in file memorizzati sull'hard disk del responsabile del procedimento o suo delegato, ma oggi in molti uffici ci si è abituati a utilizzare nel modo corretto il fascicolo elettronico e a far convergere in esso tutta la molteplice documentazione formata, raccolta e utilizzata nello svolgimento dell'iter amministrativo.

Nel contesto analogico lo sfoltimento è sempre stata una normale operazione d'ufficio, tralasciata solo nei casi in cui c'era minore attenzione alla tenuta delle pratiche. D'altro canto si tratta di un passaggio piuttosto agevole che può essere svolto rapidamente aprendo il fascicolo e sfogliando una dopo l'altra tutte le carte che vi sono contenute. In ambiente digitale l'operazione è certamente più lunga, perché la semplice consultazione di tutti i documenti può occupare molto tempo, ed è anche più complessa perché spesso richiede di confrontare fra loro file differenti e mettere ordine nel fascicolo. Aiuta aver organizzato il contenuto del fascicolo in sottofascicoli, magari riservando ad uno di essi la funzione di sedimentare i documenti che si presume di poter distruggere già alla chiusura della pratica. In ogni caso, nel contesto elettronico lo sfoltimento assume un ruolo essenziale perché alleggerisce immediatamente l'onere della tenuta dell'archivio digitale.

Va comunque detto che lo sfoltimento è una pratica estremamente delicata e presupp-

⁸ Si veda: Dimitri Brunetti, *Lo sfoltimento in archivio nel contesto della trasformazione digitale della pubblica amministrazione italiana*, in «Atlanti», vol. 31 (2021), n. 2, pp. 66-74, <https://journal.almamater.si/index.php/Atlanti/issue/view/37>

pone una accurata conoscenza della documentazione conservata nel fascicolo. Per questo motivo dev'essere realizzata solo dal responsabile del procedimento, possibilmente di concerto con il responsabile della gestione documentale, e comunque a seguito di un'appropriata formazione e sensibilizzazione sulla necessità e sui rischi dell'operazione. Tra l'altro, lo sfooltimento è l'unica azione di selezione documentale che si realizza senza l'osservanza delle procedure previste dall'art. 21 del Codice dei beni culturali per lo scarto dei documenti degli archivi.

3. La campionatura

Vi sono in archivio serie di fascicoli per le quali non sembra indispensabile provvedere alla conservazione illimitata sia in virtù del valore non significativo che della loro consistenza. Però, quegli stessi fascicoli potrebbero essere l'unica testimonianza di un'attività, di una funzione importante e quindi scartarli in maniera indistinta significherebbe perderne completamente la memoria. Si tratta spesso di serie che testimoniano il modo di operare dell'ente, ma sono troppo ampie perché sia possibile conservarle in modo completo⁹. In questi casi si può operare una campionatura all'interno della serie, così da preservare la memoria dell'azione amministrativa senza conservare illimitatamente molto materiale documentario di scarso valore.

La campionatura è una tecnica utilizzata per ottenere una rappresentazione accurata di un insieme di dati, è un processo di selezione più o meno casuale di elementi ricavati da un insieme omogeneo che si realizza prelevando dei campioni sulla base di determinati criteri (numerici, semantici, statistici ecc.) in modo che gli stessi materiali scelti risultino rappresentativi della totalità dell'insieme.

L'esigenza di ottenere un concentrato rappresentativo può essere soddisfatta con una campionatura realizzata su basi soggettive in due modi:

- la scelta di esemplari, che consiste nella selezione di una serie effimera di una o due unità con lo scopo di illustrare la prassi amministrativa ad una certa data;
- la campionatura qualitativa, che consiste nella selezione di una serie effimera di materiale specifico che è considerato di valore storico (utile quando i fascicoli di reale valore sono pochi e inseriti in serie di scarso interesse).

In presenza di serie molto uniformi la campionatura può essere fatta anche su basi obiettive:

- la campionatura accidentale o casuale, che consiste nel selezionare componenti della serie completamente a caso, applicando un metodo statistico che assicuri che tutte le parti abbiano esattamente le stesse probabilità di essere scelte (da utilizzarsi soprattutto in caso di studi statistici e di analisi quantitative);

⁹ Luciana Duranti, *I documenti archivistici. La gestione dell'archivio da parte dell'ente produttore*, Roma, Ministero per i beni culturali e ambientali, 1997, pp. 84-87. Le definizioni di campionatura sono tratte da p. 85.

-
- la campionatura sistematica, che consiste nello stabilire uno schema particolare di selezione scegliendo, ad esempio, un fascicolo ogni determinato numero di fascicoli, o tutti i materiali di un certo periodo cronologico, o tutti i fascicoli con specifiche caratteristiche all'interno di un dato periodo, o a rotazione secondo un set definito di qualità.

La campionatura sistematica è il modello che sembra adattarsi meglio degli altri nel contesto documentario di un archivio elettronico in ordine. Offre la possibilità di definire in modo obiettivo i criteri di selezione più idonei in riferimento alla funzione svolta, alla numerosità dei fascicoli e alla tipologia di materiale e di scegliere in modo consapevole le aggregazioni documentarie da mantenere. Ad esempio, per un ente che eroga contributi sulla base di bandi annuali, si può decidere di destinare alla conservazione permanente solo una percentuale dei fascicoli per ciascuna istruttoria, e se le istruttorie sono molte queste possono essere suddivise in due o più gruppi omogenei e ad essi la campionatura può essere applicata solo ad anni alterni. Rimangono però alcuni elementi da precisare: chi sceglie i fascicoli da conservare? quando? sulla base di quali criteri? e quanti fascicoli si conservano rispetto al totale? si deve dar conto dell'operazione? e dove va indicato che si fa ricorso alla campionatura?

La scelta non può essere che fatta dal responsabile del procedimento, o comunque da colui che ha istituito i fascicoli e ne conosce bene la natura e il contenuto. Nessun altro può scegliere in modo pertinente quali fascicoli conservare e quali lasciare. Ne consegue che la scelta deve essere compiuta al momento della chiusura del fascicolo, o una volta l'anno secondo un calendario prestabilito magari in relazione all'attività d'ufficio che porta alla formazione della specifica serie. In questo modo alcuni fascicoli vengono indicati come da conservare illimitatamente nel contesto di una serie che invece verrà conservata solo per un numero determinato di anni.

Però, scegliere alcuni fascicoli all'interno di una serie, seppur omogenea, può essere difficile, soprattutto se si lascia la decisione all'autonomia della persona senza fornire parametri oggettivi. La scelta delle aggregazioni documentarie potrebbe quindi essere guidata da questi criteri:

- la completezza, ovvero il fascicolo deve contenere tutti i documenti principali del procedimento;
- la significatività, il fascicolo deve poter essere assunto a modello o esempio dell'attività amministrativa e di come il procedimento è stato definito;
- la rappresentatività, ovvero il fascicolo prescelto deve essere indicativo del contenuto e della materia della serie documentale di cui manterrà memoria.

Perché la campionatura sia significativa non occorre conservare una gran quantità di fascicoli. Si selezionerà quindi un numero definito di unità, oppure di una percentuale non superiore al 5%, ma che può anche essere ridotta fino all'1%.

Naturalmente i criteri di campionatura devono essere dichiarati e indicati nel Manuale di gestione documentaria, così come in premessa al Piano di conservazione. La presenza dell'operazione di campionatura deve essere indicata nello stesso Piano in modo evidente a fianco di ciascuna voce di classificazione e, se presenti, accanto

alle aggregazioni documentarie (serie e fascicoli) ad essa associate.

Infine, va rilevato che la campionatura è un'operazione complessa che richiede di essere programmata molto bene, mantenuta stabile nel tempo, condivisa con chiarezza di obiettivi con tutti i soggetti coinvolti. Per questi motivi la campionatura è una pratica applicata assai raramente, sia nel contesto analogico che in quello elettronico, benché la sua importanza sia evidente.

CONSERVAZIONE DIGITALE: OBIETTIVI E FUNZIONE ARCHIVISTICA

Gabriele Bezzi

Abstract: Nel 2021 AgID, oltre ad aggiornare le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici pubblicate nel settembre 2020, ha pubblicato altri due importanti documenti che trattano il tema della conservazione digitale dei documenti informatici: il Regolamento che definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, fissando in un apposito allegato i requisiti generali nonché i requisiti di qualità, di sicurezza e organizzazione necessari per la fornitura del servizio e un documento di indirizzo, denominato “Progetto Poli di conservazione: definizione di un modello di riferimento per i Poli di Conservazione e la relativa rete nazionale”. Alla luce di tali novità normative, sulla base di standard internazionali e sull’esperienza conservativa sviluppata negli ultimi dieci anni all’interno del Polo archivistico dell’Emilia-Romagna (ParER), l’articolo cerca di definire la funzione archivistica della conservazione digitale partendo dall’assunto che il citato regolamento ha mantenuto come unica figura professionale necessaria il Responsabile della funzione archivistica di conservazione e che la conservazione digitale dovrà giungere a costituire, per la pubblica amministrazione, gli archivi storici del futuro e garantire, oltre ad una adeguata custodia e tutela, la piena fruizione e valorizzazione del patrimonio documentale conservato.

In 2021 AgID published three important documents: Guidelines on recordkeeping and preservation of digital records, a rule for digital preservation service and a document on preservation centre in the public sector. In the light of the new rules and based on the experience developed in ten years in ParER (digital archive center of Emilia-Romagna region), the article try to define the archival function of digital preservation and the goal to create historical archives of the future where public administration electronic records can be safely stored, in order to be accessible in the forthcoming years.

Parole chiave: Conservazione, archivistica, archivi pubblici, documenti informatici, bene culturale

Sommario: 1. Introduzione 2. Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici 3. Poli di conservazione e funzione archivistica 4. Conclusioni

1. Introduzione

Nel 2021 oltre ad aggiornare le Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, AgID ha pubblicato altri due importanti documenti che trattano il tema della conservazione digitale dei documenti informatici.

Con Determinazione n. 455/2021 del 25 giugno 2021¹ è stato adottato il Regolamento che definisce i nuovi criteri per la fornitura del servizio di conservazione dei documenti informatici, poi modificato con successiva determinazione n. 629/2021 del 16 dicembre 2021, in particolare per ciò che riguarda la piattaforma tramite cui è possibile sottoporre la domanda di qualificazione e di iscrizione nel marketplace dei servizi di conservazione gestito da AgID².

Il Regolamento integra quanto già definito nell'ambito delle Linee guida sulla formazione, gestione e conservazione del documento informatico, emanate a settembre 2020 e aggiornate a maggio 2021³, fissando in un apposito allegato i requisiti generali nonché i requisiti di qualità, di sicurezza e organizzazione necessari per la fornitura del servizio.

Composto di due allegati tecnici, il Regolamento è emanato secondo quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020 ed è entrato in vigore il 1° gennaio 2022, data a partire dalla quale è abrogata la circolare n. 65/2014.

La conservazione dei documenti informatici per conto delle pubbliche amministrazioni da parte di soggetti esterni deve uniformarsi – nel rispetto della disciplina europea – alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici nonché al sopradetto regolamento, adottati entrambi dall'Agenzia per l'Italia digitale (AgID), che segnano il superamento del precedente meccanismo di accreditamento dei conservatori.

Inoltre, in data 22 giugno 2021 AgID ha pubblicato un documento di indirizzo, denominato “Progetto Poli di conservazione: definizione di un modello di riferimento per i Poli di Conservazione e la relativa rete nazionale”⁴. Il documento è il primo esito di un tavolo di lavoro istituzionale costituito da AgID sulla base di un accordo di collaborazione con l'Archivio Centrale dello Stato, il Consiglio Nazionale del Notariato e l'Agenzia Industrie Difesa.

Successivamente al tavolo si sono aggiunti: Ministero dell'Economia e delle Finanze,

¹ Portale Trasparenza Agenzia per l'Italia Digitale - Determinazione n. 455/2021 del 25 giugno 2021 - Adozione del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lett. b). (agid.gov.it)

² Portale Trasparenza Agenzia per l'Italia Digitale - Determinazione n. 629/2021 del 16 dicembre 2021 - Modifica del Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici e relativi allegati, ai sensi dell'art. 34, comma 1bis, lett. b). (agid.gov.it)

³ Linee Guida sulla formazione, gestione e conservazione dei documenti informatici (agid.gov.it)

⁴ Definizione di un modello di riferimento per i Poli di Conservazione e della relativa rete nazionale (agid.gov.it)

Ministero della Giustizia, Direzione generale Archivi, Polo archivistico dell'Emilia-Romagna, Regione autonoma Friuli-Venezia Giulia, Regione Marche, Regione Veneto, SOGEI - Società Generale d'Informatica S.p.A., Associazione nazionale archivistica italiana.

Si sono quindi riuniti i principali soggetti pubblici che, ad oggi, risultano essere in possesso di una significativa esperienza nel campo della conservazione digitale a medio e a lungo termine per, come si legge nella notizia pubblicata da AgID il 23 giugno 2021, “promuovere e definire una rete di poli di conservazione garantendo l'interoperabilità tra gli stessi, nel rispetto del quadro normativo nazionale, delle politiche di transizione al digitale, dei criteri archivistici e degli standard di settore”.⁵ Si tratta di un documento, rivolto ai soggetti indicati nell'articolo 2 commi 2 e 3 del CAD, di indirizzo e non vincolante come gli altri due ma che offre interessanti spunti di riflessione e di analisi per approfondire quanto stabilito nelle Linee Guida, in particolare in riferimento ai rapporti con la normativa in tema di tutela dei beni culturali e della gestione della conservazione permanente di documenti e archivi destinati a far parte degli archivi storici.

Alla luce di tali novità normative, si possono fare alcune riflessioni partendo dall'assunto che il citato regolamento ha mantenuto come unica figura professionale necessaria per la fornitura del servizio di conservazione il **Responsabile della funzione archivistica di conservazione** e che la conservazione digitale dovrà giungere a costituire, per la pubblica amministrazione, gli archivi storici del futuro e garantire, oltre ad una adeguata custodia e tutela, la piena fruizione e valorizzazione del patrimonio documentale conservato.

Tali riflessioni cercheranno di giungere ad una possibile interpretazione della funzione archivistica della conservazione digitale in riferimento alla conservazione degli archivi pubblici, anche prendendo spunto dall'analisi di standard internazionali e dall'esperienza conservativa maturata negli ultimi dieci anni all'interno del Polo archivistico dell'Emilia-Romagna (ParER).

2. Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici

Il Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici del dicembre 2021 è composto da un testo di 9 articoli con una premessa e da due allegati tecnici.

⁵ <https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2021/06/23/poli-conservazione-pubblicato-il-documento-indirizzo>. Si segnala che il proseguo dei lavori di tale gruppo ha portato nel 2022 alla definizione di due ulteriori documenti, ora pubblicati nella pagina AgID sulle Linee guida: Vademecum per l'implementazione delle Linee Guida sulla formazione, gestione e conservazione dei documenti informatici e Modelli di interoperabilità tra sistemi di conservazione.

L'allegato A definisce i requisiti di qualità, sicurezza e organizzazione, tra cui la redazione di un piano di cessazione secondo lo schema riportato nell'allegato B. Ai sensi dell'articolo 8 del Regolamento, il Piano di cessazione deve essere allegato alla richiesta di iscrizione al marketplace dei servizi di conservazione e fa parte degli elementi di valutazione del possesso dei requisiti, in base alla sua conformità ai contenuti indicati nell'allegato B dello stesso Regolamento. Obiettivo primario del piano di cessazione è quello di garantire la continuità del servizio di conservazione in caso di cessazione del soggetto erogante.

Infatti, se la conservazione è l'attività volta a proteggere e custodire nel tempo gli archivi di dati e documenti informatici, è necessario garantire che tale attività possa perdurare anche oltre l'esistenza dei soggetti che erogano il servizio o degli stessi produttori dei documenti. Ciò è particolarmente rilevante nel caso di archivi pubblici, ma è importante anche nel caso dei privati, per garantire la corretta conservazione nei termini previsti dall'art. 2220 del Codice civile.

Il regolamento prevede, altresì, l'istituzione di un marketplace per i servizi di conservazione cui possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle pubbliche amministrazioni, cioè per riprendere le definizioni del Glossario di cui all'Allegato 1 delle Linee Guida i "Conservatori", ossia soggetti pubblici o privati che svolgono attività di conservazione dei documenti informatici⁶.

AgID dichiara che il marketplace non rappresenta un elenco o un albo dei Conservatori ma costituisce una vetrina dove le pubbliche amministrazioni possono individuare più agevolmente i fornitori di servizi di conservazione a norma dei documenti informatici e avviare la successiva fase di contrattualizzazione.

L'iscrizione è possibile a partire dal 01 gennaio 2022 attraverso le modalità previste dalla piattaforma dedicata, all'interno della quale il conservatore attesterà, mediante una autocertificazione rilasciata in conformità al DPR 445/2000, il possesso dei requisiti di qualità, sicurezza e organizzazione, condizione necessaria per l'erogazione di servizi di conservazione per conto della Pubblica Amministrazione.

Condizione per l'iscrizione al marketplace dei servizi di conservazione è il possesso dei requisiti specificati all'interno dell'allegato A, "Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni", del citato regolamento.

Il Conservatore interessato all'iscrizione al marketplace dei servizi di conservazione provvede a trasmettere apposita richiesta tramite la piattaforma AgID dedicata presentando la documentazione prevista, tra cui, come detto, anche il piano di cessazione previsto dall'allegato B del citato regolamento. AgID provvede all'iscrizione previa verifica formale della documentazione.

L'iscrizione non è obbligatoria, ma di fatto attesta il possesso dei requisiti necessari per erogare il servizio di conservazione alle pubbliche amministrazioni. Le ammi-

⁶ Il glossario riporta la definizione al singolare.

nistrazioni che affidano il servizio di conservazione dei documenti informatici a soggetti non iscritti al marketplace dei servizi di conservazione hanno l'obbligo di trasmettere ad AgID i relativi contratti entro trenta giorni dalla stipula affinché l'Agenzia possa svolgere le attività di verifica dei requisiti generali nonché dei requisiti di qualità, di sicurezza e organizzazione di cui all'allegato A del regolamento.

Infatti, il regolamento è stato redatto in ottemperanza di quanto previsto dall'articolo 34, comma 1-bis del decreto legislativo n. 82/2005, come integrato e modificato dal Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020, che ora stabilisce che "Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici: a) all'interno della propria struttura organizzativa; b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione."

Tale modifica era stata fatta a seguito di osservazioni provenienti dalla Commissione Europea per armonizzare la norma italiana con la vigente disciplina europea, in particolare il Regolamento UE n. 910/2014 eIDAS, nella sua attuale formulazione⁷. Alla fine del 2022 sono iscritti nel marketplace 50 soggetti tra cui Regione Toscana e Cineca dal 4/10/2022, Insiel dal 12/4/2022, Infocamere e Regione Emilia-Romagna dal 21/2/2022.

Regione Emilia-Romagna, che ha presentato domanda a firma del presidente Stefano Bonaccini già a fine gennaio 2022 è stata tra i primi iscritti nel marketplace, tutti ex conservatori accreditati.

Posso testimoniare che l'iscrizione per un conservatore già a suo tempo accreditato è abbastanza facile perché i requisiti richiesti sono molto simili a quelli previsti in precedenza per l'accreditamento e il suo mantenimento. Anzi la procedura è anche più semplice basandosi su una autocertificazione del possesso dei requisiti di cui all'Allegato A.

Cerchiamo di vedere più in dettaglio i diversi requisiti previsti. L'allegato A del regolamento distingue i requisiti in quattro categorie: requisiti generali (RG), requisiti di Qualità (RQ), requisiti di sicurezza (RS) e requisiti di organizzazione (RO).

I requisiti generali sono nove e comprendono sia aspetti specificamente tecnici di sistema, quali l'esposizione di Application Programming Interface (API) di tipo SOAP e/o REST associate alle funzionalità di versamento e esibizione (RG1) e l'integrazio-

⁷ Ora eIDAS è soggetto ad una revisione che tra gli altri interventi prevede proprio una nuova definizione di servizi fiduciari che comprendono anche "the electronic archiving of electronic documents", che potrebbe aprire scenari completamente nuovi ma non si intende qui affrontare tale aspetto in quanto non ancora consolidato in norma.

ne con SPID, o CIE o “altre identità digitali europee notificate” (RG2), che conformità a standard internazionali, quali da un lato il modello di riferimento OAIS (Reference Model for an Open Archival Information System standard ISO 14721) (RG\$) e lo standard collegato ISO 16363 (Audit and certification of trustworthy digital repositories) (RG5) e dall’altro diversi standard ETSI, quali lo standard ETSI EN 319 401, sui servizi fiduciari, con l’adozione di criteri derivanti dallo standard ETSI TS 119 511 e da tutte le norme richiamate applicabili (RG6 e RG7). È inoltre previsto, riprendendo quanto già stabilito dalle Linee guida, che la struttura descrittiva dell’indice del pacchetto di archiviazione del sistema di conservazione sia conforme allo standard nazionale UNI 11386 SinCRO (Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali) (RG 3). L’ultimo requisito generale (RG9) prevede che il Conservatore deve possedere o deve rappresentare di avere avviato il processo per la certificazione alla norma UNI 37001, «ovvero il sistema di gestione per la prevenzione della corruzione.

Vi è infine il requisito generale che prevede che il Conservatore deve possedere una descrizione del sistema di conservazione, documentando tutte le componenti tecnologiche, fisiche e logiche e le procedure per la loro gestione ed evoluzione, oltre a procedure di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche di integrità degli archivi, con l’evidenza delle soluzioni adottate in caso di anomalie, e alla descrizione delle procedure di accesso, ricerca, recupero e uso, con relativo monitoraggio degli archivi nel rispetto della normativa sulla protezione dei dati personali (RG8). Bisogna sottolineare che questo requisito, nella sua lunga formulazione, non fa altro che riprendere quanto scritto alle lettere g) ed h) del paragrafo 4.6 delle Linee Guida sul Manuale di conservazione. Quindi il requisito può essere soddisfatto dalla predisposizione del Manuale di conservazione del Conservatore, da tempo previsto per i conservatori già accreditati e ulteriormente richiesto da un requisito organizzativo (RO7), secondo quanto indicato dalle Linee Guida, con una integrazione relativa alle procedure di accesso, ricerca, recupero e uso, non così chiaramente indicate nel contenuto previsto dal citato paragrafo delle Linee guida che riprende sostanzialmente il precedente dettato della vecchie Regole tecniche sulla conservazione del 2013.

I tre requisiti di Qualità introducono invece degli aspetti di novità rispetto al precedente accreditamento quali il possesso della certificazione ISO 9001, rilasciata specificatamente per i servizi di conservazione di documenti informatici o in alternativa la certificazione ISO 20000 (RQ1), la redazione del piano di cessazione che deve dettagliare le procedure per garantire la corretta cessazione e migrazione dei servizi di conservazione secondo quanto previsto dall’allegato B (RQ2), di cui si è già trattato, e, infine, la disponibilità da parte del Conservatore a rendere disponibile su richiesta dell’AgID un account di test utilizzabile per effettuare ogni tipo di verifica che si renderà necessaria per il mantenimento della qualificazione (RQ3).

I tre requisiti di sicurezza prevedono il possesso della certificazione ISO 27001, rilasciata specificatamente per i servizi di conservazione di documenti informatici (RS1), già comunque prevista per l’accreditamento ed espressamente indicata anche nelle

Linee Guida al paragrafo 4.3 per il sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione⁸. Inoltre, il Conservatore deve sottoporre a test OWASP le componenti del sistema di conservazione avendole sviluppate in applicazione delle linee guida per lo sviluppo del software sicuro nella Pubblica Amministrazione emanate da AgID (RS2) e garantire che i servizi offerti sono soggetti ad opportuni processi di gestione della continuità operativa e di disaster recovery, specificando l'applicazione delle buone pratiche presenti nello standard ISO/IEC 22313.

Vi sono infine otto requisiti di organizzazione. Di uno è già stato accennato: il Conservatore deve possedere il manuale di conservazione comprensivo del piano di sicurezza aggiornato con la descrizione del modello organizzativo (RO7). Su questo requisito si può osservare che in precedenza i manuali dei diversi conservatori erano pubblicati da AgID ora invece per i Conservatori non vi è più una esplicita definizione di un obbligo di pubblicazione, quando invece, proprio per quanto previsto dalle Linee Guida sarebbe quanto mai necessario avere un riferimento pubblico per un documento così rilevante per i servizi di conservazione. Nel caso di una pubblica amministrazione vi è l'obbligo di pubblicare il proprio manuale di conservazione nella sezione "Amministrazione trasparente", ma sarebbe utile, come avveniva in precedenza, avere la possibilità di avere un punto certo e controllato di pubblicazione dei manuali di tutti i conservatori iscritti nel marketplace.

Gli altri requisiti di organizzazione prevedono il possesso di una polizza assicurativa con una copertura minima di € 1.000.000 per annualità assicurativa con un minimale di € 300.000 per sinistro (RO2), l'iscrizione al registro delle imprese per i soggetti privati (RO3), la garanzia di conformità agli obblighi e agli adempimenti previsti dalla normativa europea e italiana in materia di protezione dei dati personali (RO4), l'indicazione della localizzazione dei data center all'interno del territorio nazionale o all'interno della UE o extra UE, con in quest'ultimo caso l'obbligo da parte del Conservatore di effettuare una Consultazione preventiva al Garante per la privacy ai sensi dell'articolo 36 del Regolamento (UE) 2016/679 (GDPR) (RO5 e RO6) ed infine la necessità di una verifica periodica della conformità alle normative ed agli standard (RO8).

Ho lasciato per ultimo il primo requisito di organizzazione (RO1), che merita in quest'ambito un approfondimento specifico. Infatti, il requisito stabilisce che il Conservatore deve possedere le competenze necessarie per l'erogazione dei servizi di conservazione che nello specifico si definiscono nell'aver nella propria organizzazione almeno due figure professionali: Responsabile del servizio di conservazione e Responsabile della funzione archivistica di conservazione, il cui dettaglio è contenu-

⁸ Lo stesso punto delle Linee Guida chiarisce che l'aderenza agli standard ISO 27001 e ISO 14721 OASIS e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1 sono requisiti di elevato livello in termini di qualità e sicurezza necessari al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, cioè le caratteristiche che il sistema di conservazione deve assicurare in tutti i casi in cui la legge prescrive obblighi di conservazione anche a carico di soggetti privati, secondo quanto previsto dal comma 1 ter dell'art. 44 del CAD (D.lgs. 82/2005).

to in una appendice. Tale appendice riporta gli specifici profili professionali con la sintetica descrizione delle mansioni o attività associate al ruolo, ma senza riferimenti a competenze e professionalità⁹.

Per il Responsabile del servizio di conservazione si individuano mansioni relative sostanzialmente al governo complessivo del sistema di conservazione e alla corretta erogazione del servizio di conservazione nel confronto dei soggetti (enti produttori) che trasferiscono i propri documenti e aggregazioni documentali al sistema di conservazione, con la gestione anche dei rapporti contrattuali, mentre per il Responsabile della funzione archivistica di conservazione si individuano mansioni più specifiche quali la definizione e gestione del processo di conservazione, la definizione di set di metadati di conservazione, il monitoraggio del processo di conservazione e l'analisi archivistica per lo sviluppo delle funzionalità del sistema di conservazione, la collaborazione con l'ente produttore per quanto riguarda il trasferimento in conservazione dei documenti e delle aggregazioni documentali e la loro selezione, compreso i rapporti con il Ministero della Cultura che tutela e vigila gli archivi pubblici ai sensi del Codice dei Beni Culturali e del paesaggio (D.lgs. 42/2004), oltre alle modalità di "descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato" .

Scorrendo le specifiche mansioni risulta perciò evidente che per la figura del Responsabile della funzione archivistica di conservazione necessitano competenze archivistiche e che quindi sia una figura professionale che debba essere ricoperta da un archivista, cioè un professionista dotato di una formazione specifica, iniziale e continua, nell'ambito della disciplina archivistica¹⁰. Il mantenimento della necessaria presenza nell'ambito dei servizi di conservazione di una tale figura professionale rende evidente il profondo coinvolgimento dell'archivistica nel tema della conservazione di documenti informatici o in senso più ampio di archivi e informazioni digitali. Tale necessario coinvolgimento pone la professione archivistica di fronte a nuove sfide e necessari ripensamenti.

Fin dal 1983 Paola Carucci nel suo importante saggio "Le fonti archivistiche: ordinamento e conservazione", sottolineava che: "Il mutamento di supporto, il diverso modo di lettura dei dati e l'indipendenza del singolo dato rispetto al contesto in cui è inserito comportano per l'archivista nuovi problemi relativi alla conservazione."¹¹. Più recentemente Federico Valacchi scrive che "archivisti e archivistica nel nostro paese hanno iniziato a interrogarsi seriamente intorno alle nuove esigenze e pro-

⁹ Tali mansioni sono riprese dal documento sui profili professionali relativo all'ormai superato accreditamento. In tale documento i profili professionali previsti erano sei e per ognuno erano indicati anche la formazione e le esperienze minime e il tipo di rapporto contrattuale da instaurare.

¹⁰ Senza entrare in un annoso dibattito sulla formazione e la qualità della professione archivistica si rimanda allo standard UNI 11536 Figura professionale dell'archivista. Requisiti di conoscenza, abilità e competenza.

¹¹ Paola Carucci, *Le fonti archivistiche: ordinamento e conservazione*, NIS La Nuova Italia Scientifica, Roma 1983, p. 37.

spettive della conservazione, iniziando a fare i conti con la mutata fisionomia della figura professionale e con i tempi e i modi con i quali la funzione archivistica può e deve essere esercitata”¹²

Non è qui possibile esaminare l'ampia problematica e l'analisi teorica svolta all'interno della disciplina archivistica negli ultimi anni, ma si vuole solo affrontare, con particolare attenzione agli archivi pubblici e in rapporto alla normativa italiana e agli standard internazionali di riferimento, il tema di come si può declinare all'interno dei servizi di conservazione la funzione archivistica, ricordata da Valacchi.

3. Poli di conservazione e funzione archivistica

Il citato documento di indirizzo di AgID sui Poli di conservazione, oltre a presentare scenari di conservazione esistenti e tentare di dare una definizione di poli pubblici di conservazione e di una loro possibile articolazione in rete, inquadra, con ampie riflessioni, il tema della conservazione nell'ambito della normativa nazionale sottolineando che:

“La conservazione dei documenti rappresenta per le pubbliche amministrazioni una funzione di carattere istituzionale. Esse sono infatti tenute per legge a conservare i propri documenti e archivi sia come testimonianza diretta delle loro azioni al servizio della collettività che come memoria storica, in quanto gli archivi e i documenti dello Stato e degli enti pubblici sono beni culturali.

La normativa in materia di archivi e documenti pubblici è stata sempre ispirata al principio della salvaguardia della documentazione prodotta dalla pubblica amministrazione, tutelata come bene culturale e individuata come rappresentativa di atti o fatti giuridicamente rilevanti. L'obbligo di conservazione dei documenti d'archivio, oltre che indispensabile all'efficiente svolgimento delle funzioni delle pubbliche amministrazioni, è inteso a salvaguardare diritti soggettivi, interessi legittimi, il diritto d'accesso, la ricerca a fini storici, culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico”.¹³

Più avanti rileva che:

“L'attuale normativa sulla conservazione digitale non prende in considerazione, se non marginalmente, la conservazione a fini storici di documenti e archivi digitali, così come non specifica le funzioni di fruizione del patrimonio documentale, insite invece nella definizione di “archivio” data dal Codice dei beni culturali e anche dallo standard OAIS (ISO 14721).”¹⁴

Lo standard OAIS sottolinea che uno degli obiettivi fondamentali del suo modello è ampliare la comprensione di ciò che è necessario per la conservazione e l'accesso

¹² Federico Valacchi, *Gli archivi tra storia uso e futuro*, Editrice Bibliografica, Milano 2020, p. 87.

¹³ AgID, *Progetto Poli di conservazione*, giugno 2021 (d'ora in poi *Progetto Poli*) p. 8 -9.

¹⁴ *Progetto Poli*, p. 21

dell'informazione a lungo termine – cioè per un arco temporale sufficientemente ampio da essere interessato a cambiamenti tecnologici o da cambiamenti della comunità di utenti – e che per non fare confusione con le funzioni di un semplice “bit storage”, il modello definisce un Open Archival Information System¹⁵ (OAIS) che svolge la funzione di conservazione e accesso a lungo termine alle informazioni, cioè per usare le stesse parole dello standard, un Archivio, inteso come una struttura organizzata, che può essere parte di una organizzazione più grande, di persone e sistemi che accetti la responsabilità di conservare informazioni e renderle disponibili a una comunità di riferimento, o più sinteticamente, una organizzazione che mira a conservare informazioni per l'accesso e l'uso da parte di una comunità di riferimento. Lo stesso standard definisce la comunità di riferimento come un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere un particolare insieme di informazioni. La comunità di riferimento può essere composta da più comunità di utenti. Lo standard OAIS ci fornisce anche una sintetica definizione di che cosa intende per “conservazione a lungo termine” (in inglese “Long Term Preservation”), che viene così descritta: “l'azione di mantenimento delle informazioni, in una forma comprensibile in maniera autonoma dalla Comunità di riferimento e con evidenze che supportino l'autenticità, nel lungo termine”, cioè, sempre secondo la definizione dello standard OAIS, un periodo di tempo sufficientemente lungo da dover considerare l'impatto dei cambiamenti tecnologici e della comunità di riferimento. Tale periodo si estende in un futuro indefinito, quindi comprende il concetto di conservazione permanente o perenne.¹⁶

Alla luce di queste considerazioni si potrebbe aprire anche una riflessione sulla effettiva aderenza allo standard OAIS degli attuali servizi di conservazione, in particolare in tema di fruizione delle informazioni conservate ma in questa sede preme sottolineare che questi concetti in Italia sono stati spesso equiparati all'idea di conservazione permanente, cioè cercando di distinguere modelli di conservazione in rapporto al tempo di tenuta delle informazioni mentre sarebbe forse più utile valutarli in rapporto ad una diversa visione degli obiettivi che ci si pone e dei destinatari e fruitori dei servizi di conservazione. Bisogna inoltre valutare il tipo di informazioni, cioè gli oggetti digitali che si vogliono o si debbono conservare nel lungo termine,

¹⁵ Tradotto in italiano da Giovanni Michetti nel 2007 in Sistema informativo aperto per l'archiviazione ma forse si potrebbe intendere come Sistema informativo archivistico aperto, in cui il termine aperto ha un significato più di sviluppo del sistema in ambito di forum aperti e non implica che l'accesso all'archivio sia senza limitazioni.

¹⁶ Il riferimento all'autenticità è stato inserito nella versione dello standard del 2012. Lo standard fornisce anche una definizione di che cosa si debba intendere per “Comprensibile in maniera autonoma” (in inglese “*Independently Understandable*”) cioè, nella traduzione data da Michetti: una qualità propria dell'informazione che sia sufficientemente documentata per consentirne la comprensione e l'uso da parte di una Comunità di riferimento senza bisogno di fare ricorso a speciali risorse dalla disponibilità limitata (incluse le persone). Per completezza riporto anche il testo inglese: *A characteristic of information that is sufficiently complete to allow it to be interpreted, understood and used by the Designated Community without having no resort to special resources not widely available, including named individuals.*

con particolare attenzione a ciò che prescrive effettivamente la normativa italiana. Analizzando la normativa generale di riferimento, rappresentata dal CAD, con le relative regole tecniche ora definite dalle Linee Guida per la formazione, gestione e conservazione dei documenti informatici, ma, soprattutto per le pubbliche amministrazioni, anche dal Codice dei Beni Culturali, emerge chiaramente che la visione della normativa italiana, pur con i limiti sopra indicati, individua chiaramente come oggetti della conservazione i documenti informatici e le loro aggregazioni, di cui il sistema di conservazione deve mantenere caratteristiche di autenticità, integrità, leggibilità e reperibilità. Tali caratteristiche, secondo quanto stabilito dalle Linee Guida non si riferiscono esclusivamente ai documenti ma si estendono anche alle aggregazioni documentali informatiche (fascicoli e serie), con i metadati ad essi associati. Si disegna quindi un quadro maggiormente riconducibile a quelli che potremmo definire servizi archivistici di conservazione, piuttosto che soltanto ai servizi di conservazione di firme e sigilli elettronici attualmente regolamentati nella legislazione europea sulla conservazione di firme e sigilli elettronici¹⁷ e definiti negli standard ETSI specifica TS 119 511 e TS 119 512, che concentrano l'attenzione sui requisiti necessari per assicurare un servizio di conservazione qualificato delle firme elettroniche qualificate e dei sigilli elettronici che sia in grado di estenderne l'efficacia oltre il periodo di validità tecnologica, proteggendola dalla scadenza dei certificati e da debolezze crittografiche e altre questioni attinenti alle tecnologie utilizzate per la sottoscrizione.

La lettura del testo dello standard ETSI specifica TS 119 511 recante "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term data preservation of digital signatures or general data using digital signatures techniques", come scrive Giovanni Manca, "consente di comprendere immediatamente che non stiamo conservando documenti ma firme elettroniche qualificate allo scopo di estendere l'affidabilità della firma elettronica".¹⁸ Lo standard prevede che il servizio consista nel preservare nel lungo termine la capacità di convalidare una firma digitale, di mantenere il suo stato di validità e di ottenere una prova dell'esistenza dei dati firmati associati, e/o fornire prove dell'esistenza per lunghi periodi di tempo di dati generali, sia che questi dati siano firmati o meno. Sono presentati tre modelli: con o senza storage o con storage per la memorizzazione temporanea. È evidente che se è possibile svolgere tali servizi

¹⁷ Ci si riferisce in particolare al Regolamento (UE) N. 910/2014, eIDAS, considerando 61: "È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici", articoli 3, nella definizione al n. 16 dei servizi fiduciari e 34 "Servizio di conservazione qualificato delle firme elettroniche qualificata". Inoltre, tali servizi sono definiti nell'ambito degli standard ETSI specifica TS 119 511 e TS 119 512.

¹⁸ Conservazione digitale, cosa dice lo standard ETSI: le differenze con le norme italiane - Agenda Digitale. Articolo pubblicato su Agenda Digitale il 10 febbraio 2021. Si rimanda a tale testo per una prima analisi del contenuto.

anche senza memorizzazione di oggetti digitali non siamo in presenza di un effettivo sistema di conservazione destinato a ricevere e conservare nel tempo informazioni ordinate in aggregazioni.

Lo stesso standard presenta nell'Annex C, di valore informativo, una analisi delle differenze e relazioni tra due tipi di servizi di conservazione: quelli che vengono denominati "Archival services", che potremmo tradurre in servizi archivistici, sottinteso di conservazione¹⁹, e i "Preservation services" specificamente descritti nello standard medesimo. Vedendo la sintetica presentazione degli "Archival services" si capisce immediatamente che si sta individuando l'ambito in cui si muovono anche le Linee Guida Agid. In entrambi i casi ci si riferisce alle fasi dell'archivio o del ciclo di vita dei documenti: archivio corrente ("Current records") archivio di deposito ("Semi-current or intermediary records") e archivio storico ("Historical records"). Tali fasi sono esplicitamente ricordate dalle Linee Guida al punto 1.11 Principi generali della gestione documentale. Ci si muove quindi con concetti e definizioni derivati dalla disciplina archivistica e nello stesso paragrafo le Linee Guida definiscono sinteticamente che: "La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione. Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati". Come ribadisce il documento sui Poli di conservazione:

"Ai fini dell'espletamento di tale funzione, occorre che i Poli di conservazione offrano servizi che preservino sul lungo periodo i caratteri essenziali della documentazione. Occorre innanzitutto che siano in grado di conservare non solo i singoli documenti ma anche le relazioni che si instaurano fra di essi nel corso dei loro processi di produzione e di sedimentazione. Occorre cioè che siano in grado di conservare gli archivi così come si vengono strutturando all'interno dei sistemi di gestione documentale e nel corso delle successive fasi di consolidamento delle aggregazioni documentarie (ad esempio dopo l'effettuazione delle procedure di scarto). Occorre che siano in grado di gestire strutture di metadati ampie e articolate, che diano conto del contesto in cui documenti e archivi sono stati prodotti, della natura, funzioni, compiti ed evoluzione dei soggetti istituzionali che li hanno prodotti e così via. Occorre che forniscano strumenti efficienti di accesso, di ricerca, di consultazione e di

¹⁹ Si potrebbe tradurre, come fa Giovanni Manca e riprendendo la traduzione italiana di OAIS con il termine di servizi di archiviazione, ma deve essere chiaro che con tale espressione si fa riferimento alla attività di conservare il materiale documentario in modo razionale e ordinato per renderlo facilmente fruibile. Purtroppo, il termine in italiano ha spesso connotazioni negative e non è presente nella normativa se non nell'ambito del trattamento dei dati personali, non a caso derivando il termine dal Regolamento (UE) 2016/679 (GDPR), in particolare nella formulazione di "archiviazione nel pubblico interesse". Cfr. <https://www.cybersecurity360.it/legal/privacy-dati-personali/trattamento-dati-con-finalita-di-archiviazione-nel-pubblico-interesse-regole-di-conformita/> e soprattutto le Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018 (Gazzetta Ufficiale n. 12 del 15 gennaio 2019).

fruizione pubblica dei documenti e degli archivi conservati, aperti a tutti i soggetti interessati.”²⁰

Un altro elemento che fa indicare come la norma italiana pensi a servizi archivistici e non solo a quelli di preservazione della capacità di estendere la validità di firme elettroniche o digitali e fornire la prova dell’esistenza di dati per un lungo periodo di tempo²¹ deriva dalla definizione degli standard di riferimento tra i due tipi di servizi. Per i “digital archival services” in particolare lo standard OAIS e sui derivati, mentre per i “preservation service” lo stesso standard ETSI, che comunque indica che è possibile che un “preservation service” sia parte di un “archival service”, che può usarlo per fornire prova dell’esistenza dei dati basandosi su tecniche di firma digitale, ma che necessita di gestire tutti i metadati richiesti da un “archival service”. Di contro un “preservation service with storage [WST]”, può utilizzare un “archival service” per la memorizzazione dei dati. Come abbiamo visto il di OAIS è esplicitamente citato come modello di riferimento per i servizi di conservazione sia nelle Linee guida, che ne riprendono anche i principali concetti, in particolare quello di pacchetti informativi che nei requisiti previsti dal Regolamento per la fornitura dei servizi di conservazione. Se visivamente mettiamo a confronto il modello funzionale di OAIS e quello più simile tra quelli proposti dallo standard ETSI possiamo valutare immediatamente la differenza principale. Lo standard OAIS prevede un flusso di informazioni che parte dal produttore e va verso la comunità degli utenti, che può essere distinta dagli stessi produttori, mentre il modello proposto dallo standard ETSI è rivolto esclusivamente al cliente che sottopone dei documenti da verificare e validare.

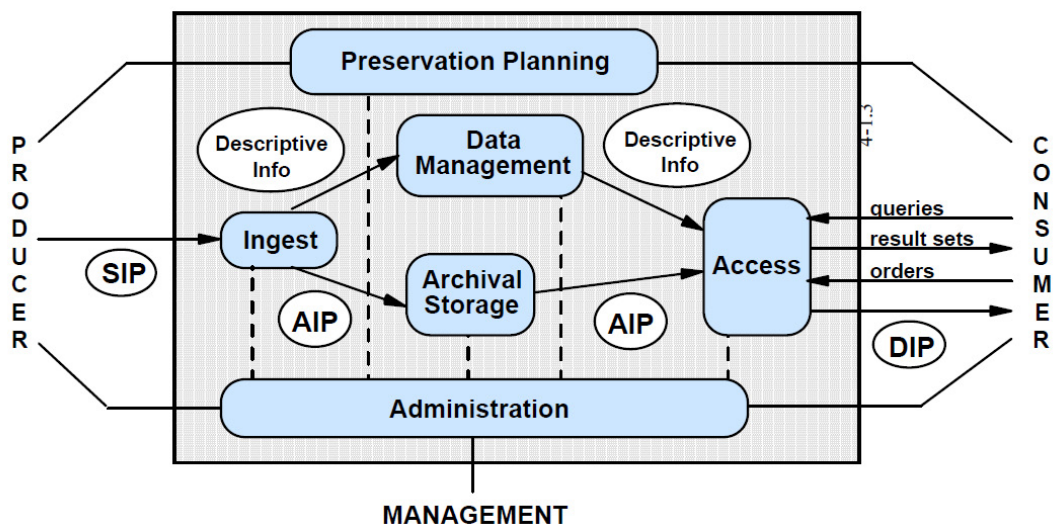


Fig. 1 Modello funzionale OAIS

²⁰ Progetto Poli, p. 22

²¹ È una libera traduzione della definizione di “preservation service” data dallo standard ETSI TS 119 511 V1.1.1 (2019-06): *service capable of extending the validity status of a digital signature over long periods of time and/or of providing proofs of existence of data over long periods of time*

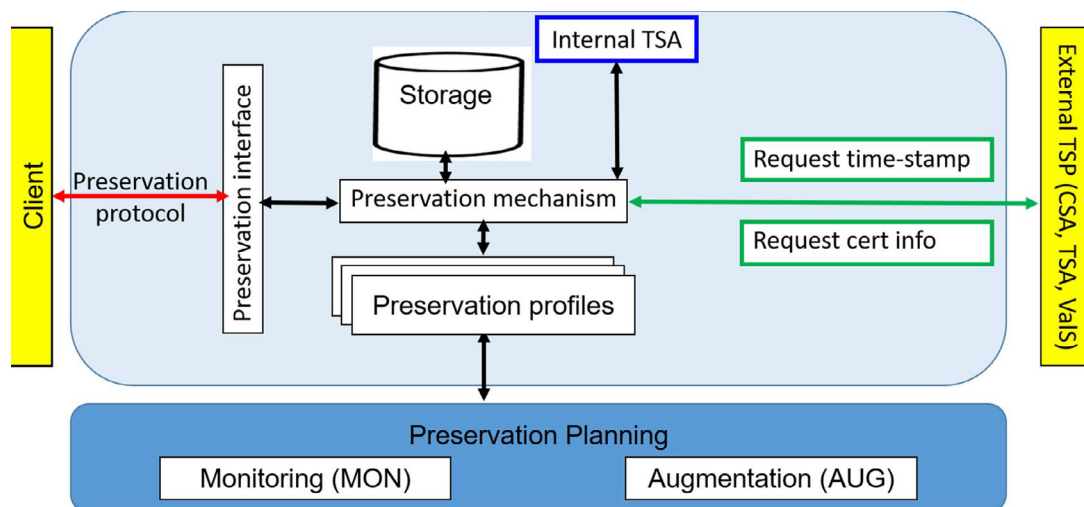


Fig. 2 Modello funzionale di un “preservation service with storage [WST]”. Da ETSI TS 119 511 V1.1.1 (2019-06), p. 15.

È vero che, nell’attuale prassi italiana, i servizi di conservazione spesso si propongono più per soddisfare le esigenze dei clienti che forniscono i documenti piuttosto che di una comunità di riferimento più ampia, ma, come abbiamo visto, ciò non è pienamente coerente con quanto prospettato dalla legislazione italiana, in particolare nel caso delle pubbliche amministrazioni, né con la visione dello standard OAIS. Credo che stia qui l’elemento caratteristico della funzione archivistica di conservazione, che può essere vista come funzione di mantenimento e trasmissione nel tempo della memoria, in particolare insita nei documenti e negli archivi informatici, per una comunità di riferimento ben più ampia rispetto ai soli produttori o possessori di documenti.

Come si legge nel citato standard UNI sulla figura professionale dell’archivista, l’attività professionale dell’archivista è mirata “a governare i complessi documentari nell’intero arco della loro esistenza, nonché a promuoverne ed agevolarne la fruizione”.

Per quanto riguarda gli archivi pubblici, nella prospettiva del modello di riferimento OAIS, il passaggio tra le diverse fasi di vita del documento o dell’archivio può essere letto in una visione di cambiamento delle comunità di utenti, cioè delle possibilità di accesso e consultabilità: la fase corrente in cui la comunità degli utenti coincide strettamente con gli uffici produttori dei documenti e delle loro aggregazioni con i loro destinatari, la fase semi attiva (archivio di deposito) in cui si può o meno estendere tale comunità ad altri interessati e la fase storica in cui, invece, la comunità degli utenti si estende a tutti coloro che vogliono accedere per motivazioni di studio e ricerca²². I sistemi e i servizi di conservazione debbono quindi essere in grado di

²² Un primo tentativo di mettere in relazione le diverse fasi dell’archivio nella visione tradizionale archivistica con i sistemi di gestione documentale e di conservazione è presente nel mio scritto

rispondere a queste variazioni nel tempo della comunità di riferimento e mettere a disposizione le informazioni conservate in modo da renderle reperibili e comprensibili in maniera autonoma ad utenti che non conoscono le modalità organizzative dei produttori dell'informazione conservata e che possono quindi non avere gli elementi originari di accesso alle informazioni stesse. Per far ciò la conservazione deve porsi come obiettivo di conservare oggetti digitali autentici, affidabili, integri, reperibili e leggibili, rendendo chiaro il contesto di produzione e provenienza e consentendo quindi il trasferimento nel tempo di memoria documentaria anche a chi non ha partecipato alla costruzione dell'informazione, ma è interessato ad usarla.

Questo è tradizionalmente uno dei punti di riflessione fondamentali della disciplina archivistica e, come abbiamo visto, uno degli scopi della professione dell'archivista che, secondo la definizione data da Isabella Zanni Rosiello, può essere visto come un mediatore di sapere. La stessa autrice ha sviluppato una riflessione sul ruolo del tempo nella valutazione del valore della documentazione scrivendo che sarebbe troppo semplicistico affermare che la documentazione archivistica nasce "amministrativa" e diventa "storica" con il mero trascorrere del tempo. "Entrambi i significati sono invece insiti nella documentazione archivistica nel momento stesso in cui è posta in essere"²³. Tale considerazione è anche alla base della definizione degli archivi e dei singoli documenti delle pubbliche amministrazioni come bene culturale fin dal momento della loro produzione.

Il Codice dei beni culturali (D.Lgs. 22 gennaio 2004, n. 42 e s.m.i.) definisce infatti senza alcuna distinzione cronologica tutti "gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico" (art. 10, comma 2 lett. b), come beni culturali, cioè testimonianze aventi valore di civiltà, facenti parte del patrimonio culturale tutelato e valorizzato in attuazione dell'art. 9 della Costituzione.

Strettamente legata a questa considerazione è anche quella sulla trasparenza della attività amministrativa e della conoscenza dell'agire pubblico come elemento di democrazia; quindi, il considerare che l'accesso libero agli archivi aumenta la conoscenza della società umana e promuove la democrazia.

In un recente intervento Gianni Penzo Doria ha ricordato e sottolineato che parlare di archivi è parlare di trasparenza²⁴.

Modelli per la conservazione e l'accesso a lungo termine degli archivi digitali e ibridi contenuto nel volume *Rete di archivi per gli archivi in rete. Conservazione e accesso ai patrimoni digitali* a cura di Gianfranco Crupi e Mariella Guercio, Roma, Edizioni ANAI, 2017.

²³ Isabella Zanni Rosiello, *Archivi e memoria storica*, Bologna, Il Mulino, 1987. Il passo è a p. 46, ma tutto il testo è una riflessione in merito poi ripresa in parte ed aggiornata anche in relazione ai sistemi informativi dell'era digitale nel volume *Gli archivi tra passato e presente* Bologna, il Mulino, 2005.

²⁴ Si fa riferimento all'intervento effettuato nell'ambito del seminario di approfondimento organizzato dalle Comunità Tematiche della Regione Emilia-Romagna a Ferrara il 27 ottobre 2022 dal titolo "*La gestione documentale motore dell'innovazione*", la cui registrazione e i materiali presentati sono reperibili alla pagina: <https://digitale.regione.emilia-romagna.it/comtem/seminari2022/la-gestione-documentale-motore-dellinnovazione>

Già nel 1997, ragionando sul destino degli archivi del “presente”, Isabella Zanni Rosiello scrive parole che rimangono quanto mai attuali:

“Forse è necessario riflettere sull’importanza degli archivi, oltre che per i relativi soggetti produttori, per altri e diversi soggetti pubblici... e per il cittadino qualunque, sia esso interessato a una pratica catastale o vittima di stragi di Stato o che intenda esercitare la propria libertà di pensiero e contribuire allo sviluppo della cultura e della ricerca, come recita il dettato della nostra carta costituzionale”²⁵.

Sarebbe quindi utile valutare anche il rapporto tra conservazione e accesso in relazione alla normativa sulla trasparenza e l’accesso civico prendendo spunto dalla frase conclusiva del citato paragrafo 1.1 delle Linee Guida:

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale, o comunque derivanti dalla normativa in materia di trasparenza, devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere i predetti obblighi, è necessario che esso garantisca la conformità di quanto pubblicato all’originale, l’autorevolezza dell’ente emanatore e del sito web, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

Questo scenario e la stessa natura delle risorse digitali può portare quindi ad anticipare nel tempo molte delle attività archivistiche che tradizionalmente erano svolte solo nella fase dell’archivio storico, attenuando la separazione tra il momento di formazione degli archivi e, per usare parole di Isabella Zanni Rosiello, “il momento in cui essi sono presi in considerazione dagli archivisti conservatori”²⁶.

4. Conclusioni

Per riassumere la funzione archivistica di conservazione potrebbe individuarsi nel “continuare a preservare, anche all’interno dei sistemi informativi dell’era digitale, i contesti di appartenenza dei documenti” per far perdurare nel tempo la loro significatività per l’intera collettività e non solo per i soggetti produttori.²⁷

²⁵ Isabella Zanni Rosiello *Che fine faranno gli archivi del “presente”?* ora in *L’archivista sul confine. Scritti di Isabella Zanni Rosiello*, a cura di Carmela Binchi e Tiziana Di Zio, Roma, Ufficio Centrale per i beni archivistici, 2000 p. 235.

²⁶ Isabella Zanni Rosiello, *Gli archivi tra passato e presente*, cit. p. 83. La stessa autrice indica che il cercare di attenuare tale separazione “non può che essere visto con favore” e aggiunge “Tale separatezza non ha favorito, spesso anzi ha penalizzato il trapasso di documentazione archivistica dall’area di uso pratico, per il quale è stata e continua a essere prodotta all’area di uso storico-culturale per il quale deve essere conservata. Gli archivisti sono consapevoli che, soprattutto nei confronti di archivi prodotti con strumenti e tecnologie informatiche è necessario non rimanere estranei alla loro produzione, se si vuole mantenere nel tempo la possibilità di reperirli e utilizzarli”.

²⁷ Loc.cit. Isabella Zanni Rosiello conclude la sua riflessione con queste parole: “Dimenticare che la documentazione archivistica è anche memoria-fonte – come spesso sembrano fare soggetti

La Dichiarazione universale sugli archivi, approvata all'unanimità dall'Assemblea generale dell'ICA - il Consiglio internazionale degli archivi, organismo mondiale di rappresentanza degli archivisti - tenutasi ad Oslo il 17 settembre 2010 e fatta propria dall'Unesco il 10 novembre 2011, riconosce infatti il ruolo degli archivisti quali professionisti dotati di una formazione specifica, iniziale e continua, che svolgono la loro funzione sociale sostenendo la creazione, la selezione e la conservazione dei documenti e rendendoli accessibili per l'uso a "tutti nel rispetto delle leggi e dei diritti dei creatori, dei proprietari degli utenti e degli individui in generale".

Tale Dichiarazione riconosce, inoltre, la molteplicità delle forme degli archivi che includono documenti cartacei, digitali, audiovisivi e di ogni altro tipo, e la necessità vitale degli archivi "per sostenere l'efficienza, la responsabilità e la trasparenza delle attività, per tutelare i diritti dei cittadini, per consolidare la memoria collettiva, per comprendere il passato e per documentare il presente al fine di guidare le azioni future". Infine, impegna a gestire e conservare gli archivi secondo modalità che ne garantiscano l'autenticità, l'affidabilità, l'integrità e l'utilizzabilità, cioè quelle caratteristiche che la stessa normativa italiana individua come finalità dei sistemi di conservazione.

Una delle funzioni tipiche della professione archivistica è quindi quella di organizzare, valutare e selezionare la documentazione per preservarne il valore e il significato trasmettendolo nel tempo di generazione in generazione.

Come scrive Federico Valacchi, la tecnica archivistica si è sviluppata proprio nel tentativo di trasformare il "molto" in "utile"²⁸. A tale scopo si sono sviluppati strumenti archivistici di governo della produzione e conservazione quali piani di classificazione, piani di conservazione, fondamentali per la selezione nel tempo e ora anche per la valutazione dei tempi di tenuta nei diversi sistemi informatici e infine strumenti di descrizione per rendere il patrimonio documentale fruibile.

In Italia la funzione archivistica di conservazione dei documenti informatici si può leggere come "la proiezione in ambito digitale di quanto previsto dal Codice dei beni culturali, in particolare dall'art. 30 comma 4, in relazione all'obbligo da parte dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché ogni altro ente ed istituto pubblico di conservare nella loro organicità i propri archivi" e di ordinarli oltre ad inventariare, cioè descrivere i propri archivi storici²⁹.

produttori, amministratori e informatici dei nostri giorni – significa voler cancellare, senza costruirne altre, una lunga e consolidata tradizione di dottrina e pratica archivistica". Si usa qui il termine "soggetto produttore" nell'accezione propria data in archivistica che identifica l'ente, la famiglia o la persona che ha posto in essere, accumulato e/o conservato la documentazione nello svolgimento della propria attività personale o istituzionale, più che in quello più specifico usato dalle Linee Guida e dallo stesso modello di riferimento OAIIS.

²⁸ Federico Valacchi, cit. p. 177.

²⁹ Per archivi storici l'art. 30 intende le sezioni d'archivio costituite "dai documenti relativi agli affari esauriti da oltre quaranta anni", ma a tal proposito si sottolinea come esempio di valore della descrizione archivistica come funzione di trasparenza la meritoria attività della Regione Lombardia che recentemente ha deciso di rendere pubblici ai cittadini i propri archivi, riordinati e inventariati, pubblicando online gli inventari relativi agli atti dell'Archivio storico (prodotti da più di 40 anni,

Traggo questo spunto dal documento di AgID sui poli di conservazione pubblicato nel giugno 2021, riflettendo che questa è l'idea da cui in Regione Emilia-Romagna siamo partiti per sviluppare un sistema, un servizio e un polo di conservazione, come si legge nell'art. 1 della Convenzione tra Regione e enti del territorio: "L'attività di conservazione svolta dalla Regione si ispira ai principi indicati dall'art. 29 del Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i., recante il "Codice dei beni culturali e del paesaggio", di coerente, coordinata e programmata attività di studio, prevenzione, e manutenzione, e si ritiene in grado di soddisfare gli obblighi in capo all'Ente produttore di conservazione di documenti informatici e in prospettiva di conservazione e ordinamento dell'archivio nella sua organicità".

Tale funzione deve certamente applicarsi all'attuale produzione digitale valutandola nelle sue diverse forme di gestione e produzione di informazioni e dati, con particolare attenzione al ruolo che i media digitali svolgono nel nostro mondo e all'uso delle piattaforme digitali da parte della pubblica amministrazione, oltre ovviamente alla tradizionale forma di produzione documentale ora gestita nativamente in digitale.

L'importanza fondamentale della conservazione digitale come irrinunciabile interesse pubblico e le difficoltà che si incontrano, sono testimoniate da un recentissimo appello di Brewster Kahle, fondatore e direttore di Internet Archive, che, a seguito dei recenti problemi di Twitter, sottolinea il bisogno delle società libere di poter accedere alla propria memoria e storia, senza che questa sia alterata dai cambiamenti di interessi politici o economici. In questo appello Brewster Kahle scrive con una certa enfasi che "la grandezza e gli scopi di Internet Archive possono sembrare qualcosa di unico ma stiamo semplicemente facendo il lavoro che le biblioteche e gli archivi svolgono da sempre: conservare e rendere accessibili la conoscenza e i patrimoni culturali. Per migliaia di anni, le biblioteche e gli archivi hanno fornito questo fondamentale servizio pubblico. Ho lanciato Internet Archive perché fortemente convinto del fatto che questo lavoro doveva essere proseguito anche in versione digitale, nell'era digitale"³⁰.

Si può specificare che solo negli ultimi due secoli, in particolare, gli archivi si sono aperti al pubblico e sono diventati fonte e strumento di democrazia ma non si può negare la necessità di proseguire questo impegno e questa funzione anche nell'era digitale.

La funzione archivistica di conservazione non è tanto quella di mantenere inalterate

quindi antecedenti al 1982) e i più recenti atti dell'Archivio di deposito, fino all'anno 2014. Chiunque potrà consultare e liberamente scaricare dal sito gli inventari, con le modalità di accesso agli atti previste nel Codice dei beni culturali e del paesaggio. Giungere con l'ordinamento e l'inventariazione fino all'anno 2014 vuol dire ampliare la concezione di valore "storico" fino a giungere alla più recente produzione documentaria, investendo quindi anche la produzione nativa digitale che, ad esempio in Regione Emilia-Romagna si può far risalire per serie organiche di atti almeno al 2009 ponendo quindi in stretto contatto e rapporto una visione tradizionale di archivio con risorse native digitali.

³⁰ L'articolo intitolato "la nostra storia digitale è in pericolo" (Our Digital History is at Risk) pubblicato inizialmente su Time e quindi il 7 febbraio 2023 sul blog di Internet Archive è stato integralmente tradotto in italiano ed è disponibile nel sito di ParER: <https://poloarchivistico.regione.emilia-romagna.it/news-in-evidenza/la-nostra-storia-digitale-e-in-pericolo>.

nel tempo le sequenze binarie degli oggetti trattati ma soprattutto quella di assicurare nel tempo la possibilità di accesso e fruizione a documentazione autentica e affidabile. In prospettiva, dunque, il sistema di conservazione e i fornitori di servizi archivistici di conservazione dovranno sempre più offrire idonee funzionalità per soddisfare le richieste di consultazione e di esibizione, in primo luogo dei produttori e sempre più in futuro dei cittadini, studiosi e altri portatori d'interesse.

Come ricorda il documento di indirizzo sui Poli di conservazione di AgID: “per i sistemi di conservazione e i conservatori diventa quindi necessario rapportarsi con le logiche di accesso e consultabilità per finalità di studio e di ricerca”³¹

Per la memoria digitale pubblica dovrà essere garantita in futuro il massimo livello di consultabilità nel rispetto delle norme sulla tutela dei dati personali e della riservatezza. In particolare, dovrà essere garantita la consultabilità dei documenti e degli archivi secondo le norme del Titolo II, Capo III del Codice dei Beni Culturali e nel rispetto delle Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate dal Garante per la protezione dei dati personali. La conservazione dovrà infatti giungere a costituire per le pubbliche amministrazioni gli archivi storici del futuro e garantire la piena fruizione e valorizzazione del patrimonio documentale conservato.

Anche in ambito digitale rimane pienamente valido e attuale quanto scritto nel 1928 da Eugenio Casanova, uno dei padri dell'archivistica italiana, nel suo testo *Archivistica*: “La conservazione degli atti in archivio...ha uno scopo positivo, ben determinato, tangibile, vale a dire quello di renderli utili alla generalità degli individui e agli individui stessi”.

³¹ *Progetto Poli*, p. 11

SEZIONE II
LA CUSTODIA DEI DATI

CUSTODIRE DATI

OVVERO STORIA DI UNA MIGRAZIONE

Monica Del Rio

Abstract [1]: L'Archivio di Stato di Venezia, nel 2005, ha reso per la prima volta disponibili online le descrizioni del patrimonio archivistico sviluppate nel corso degli anni, nell'ambito di molteplici progetti; l'anno successivo ha implementato una piattaforma attraverso cui potevano essere consultate da remoto le immagini relative ad alcuni nuclei documentari, esito delle campagne di riproduzione digitale curate dall'Istituto. Un'incredibile mole di dati messa a disposizione degli utenti; un'incredibile mole di dati minacciata dall'obsolescenza tecnologica.

Se nella gestione documentale dobbiamo pianificare opportune operazioni di riversamento, nella gestione dei sistemi informativi di questo tipo è necessario programmare puntuali attività di migrazione: custodire il dato significa riversarlo in un altro formato, significa migrarlo in un altro sistema. La migrazione è un viaggio, di cui considereremo il punto di partenza, il punto d'arrivo e quanto è stato affrontato nel mezzo per pubblicare l'attuale sistema informativo *Moreveneto*.

In 2005, for the first time ever, the State Archives of Venice made available online the descriptions of the archival holdings acquired and collected over the years and across multiple projects. The following year, it established a platform through which images relating to archival fonds could be accessed remotely. This was a result of several digital reproduction campaigns managed by the Archives. An incredible amount of data was made available to all users, data which had been at risk due to technological obsolescence. If for record management we need to plan suitable document migration of digital files from format to format, then for this type of information systems management it is necessary to program timely transfer activities: the safe keeping of data means migration to another format, it means migration to another system. Data migration is a journey: we'll examine points of departure and arrival, and everything that is tackled along the way, in the production of the current information system of the State Archives of Venice, *Moreveneto*.

Parole chiave: archivio – obsolescenza – dati- immagini – aggregazioni – descrizione - migrazione

Sommario: 1. Introduzione – 2. Il punto di partenza – 3. Il punto di arrivo - 4. La migrazione: un tracciato a due piani – 5. Non di sole termiche vive la migrazione – 6. Concludendo: siamo solo all'inizio.

¹ Questo contributo sviluppa quanto accennato in M. Del Rio, *L'Archivio di Stato di Venezia contro l'obsolescenza tecnologica* in «Filodiritto», 10 giugno 2021 (al link <https://www.filodiritto.com/larchivio-di-stato-di-veneziascontro-lobsolescenza-tecnologica>).

1. Introduzione

L'Archivio di Stato di Venezia - ASVe, nel 2005, ha reso per la prima volta disponibili online le descrizioni del patrimonio archivistico sviluppate nel corso degli anni, nell'ambito di molteplici progetti, attraverso *SIASVe*, il primo sistema informativo pubblicato online dall'Archivio di Stato di Venezia².

L'anno successivo ha implementato una piattaforma – *Divenire* – attraverso cui potevano essere consultate da remoto le immagini relative ad alcuni nuclei documentari, esito delle campagne di riproduzione digitale curate dall'Istituto³.

Un'incredibile mole di dati messa a disposizione degli utenti; un'incredibile mole di dati minacciata dal tempo.

L'obsolescenza tecnologica infatti ha inevitabilmente investito l'impianto costruito su *SIASVe* e *Divenire*, minando la possibilità di impostare un percorso di ricerca da remoto: lenta e macchinosa la consultazione delle riproduzioni digitali dei documenti a causa delle debolezze del sistema, non più aggiornato col venir meno dell'interesse degli sviluppatori; inibita la consultazione degli strumenti di ricerca otto-novecenteschi, manoscritti, riprodotti in immagine, con la dismissione di Adobe Flash Player il 12 gennaio 2021.

Per far fronte a questa minaccia e garantire la consultabilità di dati e immagini affinché ricercatori, studiosi e appassionati potessero fruire al meglio del patrimonio archivistico conservato, è stato approntato allora un programma di migrazione verso una nuova piattaforma che ha portato a *Moreveneto*, l'attuale sistema informativo realizzato grazie alle risorse stanziare dal Ministero della cultura – Direzione generale archivi per lo sviluppo informatico, impostato a partire dagli ultimi mesi del 2019, valutando *Arianna*⁴, prodotto da Hyperborea, quale software adatto a trattare e restituire la variegata mole di dati e immagini che erano di *SIASVe* e *Divenire*⁴.

2. Il punto di partenza

Per poter immaginare la situazione di partenza dobbiamo dare qualche numero.

² Per la storia del progetto *SIASVe*, curato da Claudia Salmini, si veda lo spazio dedicato nel sito istituzionale dell'Archivio di Stato di Venezia https://www.archiviodistatovenezia.it/images/file-pdf/SIASVe_STORIA.pdf.

³ Per la descrizione del progetto *Divenire* si veda lo spazio dedicato nel sito istituzionale dell'Archivio di Stato di Venezia https://www.archiviodistatovenezia.it/images/file-pdf/Progetto_DIVENIRE_storiaDALsito.pdf.

⁴ I dati sono stati migrati nella piattaforma *Arianna*, di Hyperborea; *moreveneto* è stato inaugurato il 10 giugno 2021 ed è costantemente aggiornato. Il progetto è stato curato da chi scrive, con la collaborazione Andrea Erbo e Pier Paolo De Minicis (colleghi dell'Archivio di Stato di Venezia) e Daniela Villani, Antonella Ghisaura e Marcello Serenetti (di Hyperborea); si è avvalso dei fondi della Direzione Generale Archivi – Ministero della Cultura e ogni scelta è stata sostenuta dall'allora nostro Direttore, Gianni Penzo Doria.

SIASVe contava 14.474 schede di complessi archivistici (fondi complessi, fondi, serie, etc.), 1.228 di unità archivistica, 1.581 di soggetto produttore, 954 di strumenti di ricerca, alle quali si aggiungevano 37.968 immagini in formato jpg e 102 file in formato pdf.

Le schede di descrizione erano di quattro tipi:

- complesso archivistico;
- unità archivistica, con possibilità di allegare immagini;
- soggetto produttore;
- strumento di corredo, con possibilità di allegare immagini e pdf.

Divenire raccoglieva 121.280 immagini in formato tiff (400 dpi), tiff piramidale (300 dpi) e jpg (400 dpi); alcune di queste condivise con *SIASVe*, altre gestite dall'origine in *Divenire*⁵ o migrate da sistemi precedenti, legate a progetti di digitalizzazione diversi⁶, che prevedevano schede di descrizione differenti in relazione alla tipologia documentaria trattata, fossero pergamene notarili o pontificie, disegni, dichiarazioni di *decima* o documenti turchi.

3. Il punto d'arrivo

Tutto questo – dati e immagini – doveva essere conservato e reso disponibile per la consultazione da remoto; tutto questo doveva migrare in *Arianna4*, software a due facce, una per l'archivista (*Arianna for Work – Arianna4W*) e una per l'utente (*Arianna for View – Arianna4V*), e a più moduli, alcuni dei quali veicolanti le possibilità di offrire all'utente modalità di ricerca differenziate⁷.

Arianna4 incarna la logica della descrizione multidimensionale⁸ e prevede schede di descrizione per:

- aggregazione logica (*alias* complesso archivistico);
- unità archivistica, con possibilità di scegliere le più specifiche scheda cartografica, scheda F o scheda OAC; questo è l'unico livello a cui è possibile allegare un *oggetto culturale* ossia un'immagine o file di testo in formato pdf

⁵ Si veda, per esempio, il progetto *Decime 1514* realizzato con il sostegno della Fondazione Hedgelawn, Maryland – USA (2012).

⁶ Si vedano per esempio il progetto europeo Med-Arces (2000) e progetto ASMM. Archivio Storico Multimediale del Mediterraneo (2003).

⁷ La versione attualmente utilizzata per *Moreveneto*, conta sul *modulo immagini* che permette l'accesso attraverso la *Galleria* e il *modulo accesso per entità*, che permette la visualizzazione in homepage delle sfere di diverso colore e dimensione, che rappresentano le entità.

⁸ Si vedano *A conceptual model for archival description (draft v0.1, september 2016). Il contributo italiano. RECORDS IN CONTEXTS*, «Il mondo degli Archivi. Quaderni», n. 2, 2017; G. Michetti, *I sei lati del mondo. Una topologia per esplorare il territorio dei beni culturali in Ritrovarsi nel contesto: le entità come luogo di incontro fra discipline*, convegno online promosso da Sapienza Università di Roma e Biblioteca nazionale centrale di Roma, 5 novembre 2021 (al link https://www.youtube.com/watch?v=pAnmW4-Zz08&list=PL-iQNAYINN_GQ-xuV9svNA3MACSaA4xTl&index=3).

visualizzabile dall'utente;

- entità, ovvero organizzazione (*alias* ente), persona, famiglia, luogo, evento, cosa notevole, potenzialmente collegate ad aggregazioni logiche, unità archivistiche e tra loro, secondo relazioni definite e specifiche, che possono moltiplicarsi all'infinito.

In un'altra area di descrizione (*aggregazioni fisiche*) si ricostruisce la mappa topografica dei depositi per fissare la collocazione dei pezzi (il *topografico*). A questa rappresentazione ad albero, strutturata gerarchicamente dalla sede allo scaffale, si collegano le schede di descrizione di aggregazioni logiche e unità archivistica nell'implementazione del campo *collocazione fisica*.

4. La migrazione: un tracciato a due piani

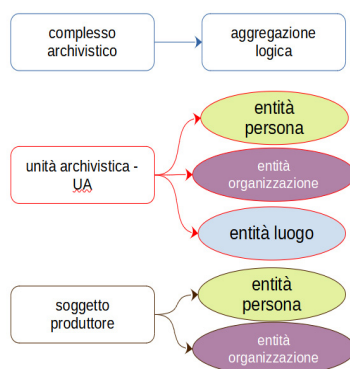
L'analisi propedeutica alla migrazione è stata quindi impostata su due piani, osservando la struttura complessiva dei due sistemi precedenti e studiando il tracciato record per ciascun livello e per ogni tipo di scheda, al fine di disegnare con esattezza il trasferimento dei dati nei campi pertinenti. Da un lato la base costituita per *SIASVe* come per *Arianna4* dagli standard internazionali di descrizione – ISAD-G e ISAAR-CPF – ha permesso un allineamento naturale, dall'altro però, quando si è aperta la tela fatta di entità e relazioni, si è resa necessaria una ristrutturazione delle informazioni.

Infatti, mentre partendo dalle schede di descrizione-complesso archivistico di *SIASVe* è stato possibile aprire la scheda di descrizione-aggregazione logica di *Arianna4* procedendo alla mappatura dei dati e alla verifica dei campi, per molte delle schede di descrizione-UA, al fine di recuperare in modo efficace le informazioni, non è stato sufficiente aprire la scheda-unità archivistica, ma si sono dovute contestualmente associare una o più scheda-entità (persona, famiglia, organizzazione e/o luogo) secondo specifiche relazioni, determinate dalla natura del campo della scheda d'origine.

Un ripensamento è stato richiesto anche per le schede di descrizione degli strumenti di corredo, sebbene la soluzione sia risultata obbligata: la scheda UA è in *Arianna* la sola in grado di ospitare un *oggetto culturale*, ossia un'immagine o file di testo in formato pdf visualizzabile dall'utente, per questo motivo è risultata essere l'unico spazio in cui poter migrare i dati di descrizione degli strumenti di ricerca associati alla riproduzione in immagine di quelli manoscritti o al file di testo in formato pdf. Sono stati dunque creati dei livelli denominati *strumenti di corredo*, che compaiono *in primis* nella struttura ad albero; a questi sono agganciati come UA i singoli strumenti di ricerca.

Spontaneo è stato il percorso di migrazione di quelle che erano le schede di descrizione dei soggetti produttori in *SIASVe*: da ogni scheda si è aperta una scheda-entità organizzazione, persona o famiglia secondo il tipo originario ed è stata

collegata all'aggregazione logica secondo il legame preesistente, semplicemente definendo la relazione è *produttore*.



L'acquisizione del patrimonio conservato in *Divenire* è risultata più laboriosa, proprio perché quando le immagini erano corredate da schede, queste, impiantate su progetti diversi, non presentavano una matrice comune bensì peculiarità legate alla tipologia documentaria che descrivevano. Ognuna ha richiesto un trattamento proprio.

Le schede relative a pergamene, condizioni di decima e documenti turchi hanno aperto schede-UA collegate ad un numero variabile di schede-entità. Nel dettaglio, per la scheda di descrizione delle pergamene, sono state generate:

- dal campo *data topica* una scheda-entità luogo, legata dalla relazione *data topica*;
- dal campo *notaio* una scheda-entità persona, legata dalla relazione *notaio*;
- dal campo *testimone* una scheda-entità persona, legata dalla relazione *testimone*.

Così per la scheda descrittiva della condizione di decima, sono state generate:

- dal campo *data topica* una scheda-entità luogo, legata dalla relazione *data topica*;
- dalla somma dei campi *dichiarante-nome (forma normalizzata)* e *dichiarante-cognome (forma normalizzata)* una scheda-entità persona, legata dalla relazione *dichiarante*. In questa scheda a partire dai campi originari *patronimico* e *qualifica*, sono stati implementati i campi *altre denominazioni/patronimico* e *qualifica*.

Dalla scheda di descrizione dei documenti turchi⁹ si è scelto di estrarre solo una scheda-entità luogo dal campo *data topica* originario, specificando questo legame nella relazione.

Sono invece state aperte schede cartografiche per mappe afferenti al cosiddetto catasto austriaco e disegni appartenenti a fondi archivistici diversi.

Poiché le mappe sono state ereditate da Med-Arces, primo progetto di digitalizzazione

⁹ Questo fondo archivistico è descritto nel dettaglio in A. Bombaci – M.P. Pedani, *I documenti turchi dell'Archivio di Stato di Venezia*, Roma Ministero per i beni culturali e ambientali, Ufficio centrale per i beni archivistici, 1994 (<http://www.archivi.beniculturali.it/dga/uploads/documents/Strumenti/5156eece7a3c.pdf>)

affrontato dall'Archivio di Stato di Venezia che non prevedeva una vera e propria scheda descrittiva, i soli campi recuperati per la scheda cartografica sono *denominazione, tipologia di rappresentazione e altra segnatura*.

Diversamente, a partire dalla scheda di descrizione dei disegni, si sono aperte:

- dal campo *data topica* una scheda-entità luogo, legata dalla relazione *data topica*;
- dal campo *autore* tante scheda-entità persona, legata dalla relazione *autore*, quante erano le occorrenze nella scheda d'origine.

L'automatismo che genera schede entità a partire da un determinato campo di una scheda di descrizione porta con sé un problema: ognuno di questi determinati campi darà origine ad una scheda, ossia se n campi *notaio* di n schede-UA sono implementati dal valore *Albertus Magnus*, avremo n schede entità-persona intestate ad *Albertus Magnus*, dal momento che non è possibile decidere a priori se si tratti di omonimia o della stessa persona. Di qui la necessità di una verifica a posteriori finalizzata all'accorpamento delle schede che si riferiscono alla stessa entità.

5. Non di sole termiche vive la migrazione

La proliferazione delle schede entità non è l'unico problema che si è posto nel percorso di migrazione. L'analisi propedeutica ha fatto emergere delle linee di criticità dove già *SIASVe* e *Divenire* avevano optato per dei compromessi volti ad acquisire modelli di dati derivanti da progetti precedenti oppure presentavano delle peculiarità proprie della loro struttura informativa; dove l'architettura di *Arianna*⁴ richiedeva di creare relazioni che non esistevano in origine oppure di trasformare quelle che *SIASVe* costruiva in modo non replicabile nel nuovo sistema.

La scheda descrittiva del complesso archivistico di *SIASVe* ereditava tutti i dati raccolti dal progetto *Anagrafe informatizzata degli archivi italiani* (1997-2000), che in un'unica rilevazione organizzava le informazioni relative a nucleo archivistico e soggetto produttore, cosicché in *SIASVe* trovavamo i soggetti produttori nel campo duplicabile *altra denominazione* specificato da *tipologia-provenienza*, dal quale in un secondo momento venivano ricavate le schede-soggetto produttore. Nello stesso campo, con *tipologia-Guida generale degli archivi di Stato* e *tipologia-Da Mosto*, troviamo sempre la denominazione tratta da questi tradizionali strumenti di ricerca, anche quando coincide con l'intestazione della scheda di descrizione del complesso archivistico.

Questo in *Moreveneto* ha comportato un moltiplicarsi non pertinente delle occorrenze del campo *altra denominazione* e richiederà un inevitabile intervento di revisione. D'altro canto, invece, *SIASVe* prevedeva una sezione composta da sei campi, ognuno destinato a contenere il codice numerico identificativo dei livelli superiori e del livello della scheda stessa, quindi per esempio nella scheda relativa alla sottoserie avremmo avuto compilati tre campi, per fondo, serie e sottoserie con una risultante uguale a *001.001.001*, fotografia della relazione gerarchica tra i livelli, che mantenendo anche

la granularità dell'informazione rende possibili ricerche e riordinamenti anche su un solo specifico livello.

Arianna4 esplicita la relazione tra i livelli esclusivamente nella struttura ad albero e il codice identificativo del livello può essere utilizzato per il riordino del livello superiore solo se, bluffando, si inserisce nel campo *indice di classificazione*.

Relazioni *ex novo* devono essere invece create non solo quando si generano nuove schede entità che richiedono la definizione di uno specifico legame tra loro o con il complesso archivistico, ma anche nel momento in cui dalla scheda di aggregazione logica o unità archivistica, per indicare la collocazione dei pezzi archivistici che la costituiscono, si crea il link che punta alla sezione *aggregazioni fisiche* nella struttura ad albero articolata in sede, piano, area, fino ad indicare almeno la stanza in cui questi sono conservati.

6. Concludendo: siamo solo all'inizio

Questi sono solo alcune delle sfide che sono state affrontate, scegliendo di custodire i dati attraverso una migrazione.

Il primo obiettivo è stato raggiunto: tutti i dati e le immagini che erano in *SIASVe* e *Divenire* sono salvi e ora gestiti e conservati in *Moreveneto*. Devono essere verificati, devono essere *reducti ad unum* laddove si sono indebitamente moltiplicati, devono essere sempre resi in modo tale da ampliare le possibilità di ricerca offerte all'utente. L'impegno è attualmente indirizzato a questo. Ma non solo.

Molte delle potenzialità di *Arianna4* sono ancora da sondare: oltre a quello puntellato dalle entità, un terreno di sperimentazione è quello costituito dai moduli di import ed export.

È possibile infatti modellare una tabella con campi propri, selezionati da quelli che costituiscono le schede descrittive – siano esse di aggregazione logica, unità archivistica o entità – così raccogliere dati in modo massivo o mutuandoli da descrizioni già esistenti, ma non strutturate. Il file risultante, in formato csv, contenente la tabella può essere importato al livello pertinente nella struttura ad albero già presente.

Altra area di sperimentazione è legata all'interoperabilità: non si può pensare di essere custodi accorti, se non si dialoga con le piattaforme nazionali, attraverso standard e modelli per descrizione e metadattazione promossi dall'ICAR, l'Istituto centrale per gli archivi.

Arianna4 prevede un modulo di esportazione chiamato appunto *interoperabilità-ICAR*, da cui si ricava un file xml. Stiamo testando la possibilità di estrarre da *Moreveneto* i dati descrittivi attraverso questo modulo, al fine di riversarli in *Archivio Digitale* o in quella che sarà la nuova piattaforma nazionale che come punto di accesso unico al patrimonio archivistico nazionale potrà diventare il privilegiato e quindi il luogo più efficace in cui impostare una ricerca che non coinvolga solo l'Archivio di Stato di Venezia.

Ma questo è un altro progetto e sarà un altro viaggio da raccontare.

LA CUSTODIA DEI CONTENUTI NELLA SOCIETÀ DELL'INFORMAZIONE: OSSERVAZIONI SULLA SENTENZA CGUE C-460/20

Enrico Pelino

Abstract: Custodire contenuti digitali è un'attività chiave sia nel contesto di un'organizzazione imprenditoriale o di un ente pubblico sia in quello più ampio della società dell'informazione, forse a maggior ragione in quest'ultima, dove l'informazione ha rilievo, appunto, strutturale. Anche nell'ecosistema più ampio dell'informazione, si pongono criticità in parte analoghe a quelle che emergono in sede di conservazione sostitutiva o digitale, quali l'esigenza di individuare ruoli precisi con funzioni di custodia e quelle di assicurare l'integrità dell'informazione, la sua organizzazione (discutendone i criteri), la sua accessibilità.

Ma non si danno ruoli senza responsabilità, e la recente tendenza giuridica nella società dell'informazione si muove proprio nel senso di mitigare la tradizionale (e ancora oggi ribadita) posizione di neutralità degli intermediari, precisandone sempre più gli obblighi di diligenza. La tendenza è ben delineata nel recente Digital Services Act (DSA) ma appare emergere anche in decisioni giudiziarie basate sul GDPR. Una recente sentenza della Corte di giustizia dell'Unione europea fornisce, in proposito, un interessante caso concreto che sembra anticipare più sottili approfondimenti verosimilmente attesi nel prossimo futuro, quando il DSA, una volta pienamente applicativo, comincerà a produrre contenzioso. Ma in che senso l'intermediario dell'informazione può essere considerato un soggetto che svolge professionalmente un ruolo di custodia dei contenuti digitali? E la sua diligenza quali limiti deve incontrare per non divenire attività nociva di manipolazione?

Preserving digital content is a key activity both in the context of a business organisation or a public body and in the broader context of the information society, perhaps all the more so in the latter, where information is indeed of structural importance. In the broader information ecosystem, critical issues arise that are in part similar to those that emerge in the substitutive or digital storage industry, such as the need to identify well defined roles with custodial functions, and those of ensuring the integrity of the information, its organisation (and criteria), its accessibility.

But there are no roles without responsibilities, and the recent legal trend in the information society is moving precisely in the direction of mitigating the traditional (and still reaffirmed) position of neutrality of intermediaries, by increasingly specifying their obligations of due diligence. The trend is well outlined in the recent Digital Services Act (DSA), but also appears to be emerging in judicial decisions

based on the GDPR. A recent ruling by the Court of Justice of the European Union provides an interesting case in this regard, which seems to anticipate more subtle insights likely to be expected in the near future, when the DSA, once fully applicable, will begin to produce litigation. But in what sense can an information intermediary be considered a subject professionally performing a role of “custodianship” of digital content? And what limits must its due diligence obligations meet in order not to result in a harmful intervention on information?

Parole chiave: società dell’informazione, intermediari, controllo dell’informazione, diritto di cancellazione, GDPR, DSA, neutralità/intervento sui contenuti.

Sommario: 1. Il contesto – 2. La vicenda – 3. L’intermediario come “professionista” della custodia? – 4. Conclusioni.

1. Il contesto

La custodia delle informazioni è il tema del presente numero monografico, mi sia consentito di esaminarlo secondo una prospettiva alquanto diversa da quella degli altri contributi di questa raccolta, in chiave cioè di protezione dei dati personali e più precisamente di cancellazione di dati personali nel contesto di società dell’informazione, dunque di art. 17 GDPR.

La richiesta di cancellazione è propriamente un’attività di alterazione del panorama informativo, perché interviene materialmente sullo stesso, sottraendone contenuti.

Del resto, il potere dell’interessato del trattamento è appunto definito quale controllo sull’informazione (nei limiti in cui essa lo riguarda, e in bilanciamento con altri diritti). E il controllo implica, concettualmente, l’intervento materiale sui contenuti.

Lo spunto è la recente sentenza della Corte di Giustizia europea dell’8 dicembre 2022 sul caso *Tu e Re c. Google LLC*, C-460/20.

La pronuncia si propone anche come occasione per una riflessione più ampia sul ruolo degli intermediari della società dell’informazione, tema quanto mai attuale in seguito all’approvazione del Digital Services Act, reg. (UE) 2022/2065.

Siamo dunque al centro della polarità tra conservazione e rimozione di elementi conoscitivi nell’ecosistema dell’informazione digitale. E, com’è noto, in questa tensione giuridica gioca un ruolo chiave l’intermediario, ossia, potremmo dire con una definizione appena sgrossata, un soggetto che presta un servizio di organizzazione e reperibilità dell’informazione.

Ai fini della pronuncia citata, ci interessa quel particolare intermediario che svolge attività di motore di ricerca. Il motore non custodisce direttamente i contenuti digitali ma custodisce, e soprattutto organizza, la mappa dei link a tali contenuti e le relative chiavi di ricerca. La richiesta di cancellazione dei dati personali è perciò necessariamente limitata, nei confronti di tale tipologia di intermediario, ai link.

Va notato del resto che la deindicizzazione soddisfa spesso le ragioni dell’interessato, ossia dal soggetto a cui l’informazione si riferisce, senza che sia sempre decisivo

ottenere la più radicale rimozione dell'informazione dai siti degli editori, esito talvolta neppure giuridicamente conseguibile.

Ciò perché l'elemento determinante per l'accesso e l'utilizzabilità dell'informazione sta nella sua organizzazione e nella sua reperibilità agevole, non tanto nella mera esistenza in un qualche punto del sistema. Come esattamente rilevato da Cass., Sez. I, 8 febbraio 2022, n. 3952: *“La deindicizzazione asseconda il diritto della persona a non essere trovata facilmente sulla rete (si parla in proposito di right not to be found easily)”*.

Ma veniamo al caso e alla soluzione che ne ha dato la Corte di giustizia.

2. La vicenda

La vicenda contenziosa è delle più classiche. L'interessato o gli interessati, nella specie due soggetti che rivestivano cariche sociali all'interno di un gruppo, chiedevano la rimozione dall'elenco dei risultati di ricerca di articoli sul proprio conto e di foto. Nonostante nella sentenza affiorino dubbi sulla reale portata informativa di questo materiale, possiamo considerare gli articoli come connotati da interesse pubblico, perché viene evocato il bilanciamento tra diritto all'informazione e tutela della sfera privata, in definitiva la classica contrapposizione cronaca/privacy.

Questa volta la rimozione non si basa sul passaggio del tempo e sul corrispondente affievolimento dell'interesse pubblico alla conoscenza, ossia sull'oblio, ma sull'asserita inesattezza delle informazioni, ossia su una mancanza di qualità necessarie. Non che questo abbia realmente rilevanza, il diritto evocato è pur sempre quello riconosciuto dall'articolo 17 GDPR.

I passaggi della decisione che qui veramente ci interessano sono quelli riguardanti il ruolo del motore di ricerca. Il tema è quello di stabilire fino a che punto e con quanta autonomia sia possibile per il motore decidere quali notizie tenere e quali cancellare, a seguito di richiesta dell'interessato.

È, se vogliamo, anche il tema dominante del DSA: quando si è responsabili della permanenza/rimozione dei contenuti illeciti e quali sono i connessi obblighi di diligenza? Il che schiude alla domanda principale, non affrontata direttamente (o comunque soddisfacentemente) dal DSA: chi stabilisce, e sulla base di quali elementi, se i contenuti sono illeciti e quindi da rimuovere, quando sul punto non si sia ancora pronunciata un'autorità giudiziaria o non sussista un ordine amministrativo?

Come si vede, l'argomento, così posto, diventa perciò subito coinvolgente, perché raggiunge profili connessi con la circolazione delle idee e del dissenso, con la costruzione della dialettica democratica, con la trasparenza e con l'alterazione deliberata del patrimonio informativo, con il ruolo proattivo o neutrale degli intermediari della società dell'informazione, ossia di quelle forze che in ultima analisi plasmano l'attingibilità di contenuti digitali nella Rete.

La Corte di Giustizia già in passato, nello storico arresto Google Spain SL, C-131/12,

del 13 maggio 2014 aveva sfiorato la questione, ma senza realmente affrontare i limiti dell'iniziativa dell'intermediario nella scelta di rimuovere contenuti, in assenza di un ordine giudiziale o amministrativo. In quell'occasione, al Giudice era bastato tracciare un criterio generale di prevalenza della sfera personale sia sull'interesse economico del motore di mantenere l'indicizzazione sia su quello generale del pubblico a fruire di un quadro informativo integro.

Ora invece viene toccato il problema dell'ampiezza del ruolo decidente che siamo disposti o no a riconoscere al motore sulle informazioni da tenere, da modificare o da eliminare nella ricerca generalista.

Sia chiaro, l'intermediario non è e non è mai stato un soggetto neutrale rispetto all'informazione. Il posizionamento dei link nella lista dei risultati di ricerca o l'ordine e il contenuto del feed di una piattaforma *social* sono il risultato dell'applicazione di algoritmi proprietari, che hanno un'incidenza fortissima sulla visibilità o invisibilità di informazioni, fino a creare in casi estremi vere e proprie *filter bubble*, ossia personalizzazioni ripetitive di contenuti del medesimo tenore, dunque manipolanti. Tuttavia, nel caso che ci occupa, ci spostiamo evidentemente a un livello più profondo e radicale rispetto alla semplice gestione del posizionamento di informazioni.

3. L'intermediario come “professionista” della custodia?

Il pericolo è chiaramente evidenziato dalla Corte, che nota come *“sussisterebbe un rischio reale di effetto dissuasivo sull'esercizio della libertà di espressione e di informazione se il gestore del motore di ricerca procedesse a una deindicizzazione [...] in modo pressoché sistematico”*.

Più esattamente, si pone *“un serio rischio che siano deindicizzati contenuti che rispondono ad una legittima e preponderante esigenza di informazione del pubblico e che divenga quindi difficile trovarli in Internet”*.

Ciò, secondo la CGUE, potrebbe accadere se si dovesse ravvisare per i motori di ricerca di *“un obbligo di indagare sui fatti e di organizzare, a tal fine, uno scambio in contraddittorio, con il fornitore di contenuto, diretto ad ottenere elementi mancanti riguardo all'esattezza del contenuto indicizzato. Siffatto obbligo, infatti, poiché costringerebbe il gestore del motore di ricerca stesso a contribuire a dimostrare l'esattezza o meno del contenuto menzionato, farebbe gravare su tale gestore un onere che eccede quanto ci si può ragionevolmente da esso attendere alla luce delle sue responsabilità, competenze e possibilità”*.

Nonostante questo, come vedremo, la Corte non esonera l'intermediario dalla valutazione autonoma (ossia non basata su ordine giudiziale o amministrativo) circa l'illegittimità dei contenuti. E il punto è interessante perché segna il passaggio sempre più evidente da un ruolo completamente neutrale a un ruolo responsabilizzato,

nel quale è più definito, ed entro un certo limite, espressamente richiesto, l'obbligo di prendere decisioni sulla conservazione o alterazione del patrimonio informativo. In particolare, il Giudice dell'Unione ha ritenuto corretto impostare il bilanciamento nei termini che seguono:

- . l'interessato del trattamento, ossia colui che promuove la richiesta di cancellazione, non è tenuto a motivarla con un previo provvedimento giudiziale che riconosca l'illiceità del contenuto, tuttavia ha l'onere di fornire all'intermediario, nella specie al motore di ricerca, evidenze ragionevoli a supporto della sua richiesta;
- . il motore non è gravato di alcun ruolo attivo nella ricerca di evidenze contrarie; tuttavia, è tenuto a esaminare quelle presentate dall'interessato e, ove siano convincenti, procedere alla rimozione del contenuto.

La soluzione appare forse più salomonica che soddisfacente, ma costituisce un punto di partenza in una direzione di accresciuta responsabilizzazione degli intermediari.

4. Conclusioni

Esaminando il concetto di custodia dei contenuti digitali nel contesto della società dell'informazione, se ne evincono alcuni tratti connotanti e originali.

Innanzitutto, l'esatto punto di caduta delle regole appare in qualche misura mobile e tende a essere aggiornato e precisato dalla giurisprudenza.

La società dell'informazione è allo stesso tempo un ecosistema in cui è desiderabile disporre di informazione completa, non alterata e accessibile, e contemporaneamente si pone l'esigenza opposta di ottenere la rimozione, il filtro, l'inaccessibilità o la più difficile accessibilità di alcuni contenuti.

Questo si verifica per varie ragioni. Per esempio, perché la società dell'informazione è anche la società della troppa informazione, e si è scoperto che la troppa informazione è di ostacolo allo sviluppo individuale (diritto all'oblio). Ma si verifica anche perché la società dell'informazione è anche, in misura più o meno ampia a seconda delle fonti e dei contesti, la società dell'informazione inesatta (come nel caso esaminato) o comunque incompatibile con le regole del diritto.

Dinanzi a iniziative di deliberata manipolazione (*fake news*), la manipolazione opposta (rimozione di contenuti *fake*) diventa paradossalmente il modo di assicurare l'esattezza dell'informazione. E tuttavia, decidere che cosa sia *fake news* conduce su un terreno estremamente scivoloso, specie se la decisione è rimessa agli stessi intermediari. Il punto delicato è cioè che lo stesso concetto di informazione esatta da preservare appare controverso.

Dal febbraio alla metà di maggio 2021 Facebook censurava informazioni che ipotizzavano l'origine di laboratorio del virus "Sars-CoV-2", poi, con il mutare di posizioni nella politica americana, tali informazioni sono state non solo riammesse ma considerate, nel contesto generale dei media, perfino poziori (cfr. Alex Hern, *Facebook*

lifts ban on posts claiming Covid-19 was man-made, in *The Guardian*, 27.5.2021¹). La disponibilità di informazioni ne è risultata significativamente alterata, e non in conseguenza dell'esercizio di diritti, come nel caso esaminato dalla Corte di Giustizia, ma per scelte adottate *motu proprio* da una piattaforma su temi altamente controversi, ma a maggior ragione preziosi per il dibattito pubblico. È sui temi controversi che si dibatte, non su quelli di unanime convergenza.

Il punto è che, nella società dell'informazione, i custodi dell'organizzazione e della reperibilità di contenuti, che in buona misura sono intermediari dell'informazione, occupano un ruolo che è contemporaneamente decisivo e segnato da grande fragilità. Spostandoli da un ruolo di neutralità nella custodia a un ruolo attivo e decisionale, si rischia di chiedere loro di volta in volta troppo o troppo poco. Chi scrive è convinto che il coinvolgimento diretto degli intermediari, ad esempio (come abbiamo visto) nel riscontro all'esercizio di diritti dell'interessato al trattamento sia auspicabile e già perfettamente costruibile secondo le regole attuali, è tuttavia certo che la gran parte degli altri scenari di gestione della fruibilità dell'informazione va ancora accuratamente studiata, con freddezza e liberi da smanie emergenziali.

Prevedibilmente, questa sarà anzi proprio una delle aree di maggior interesse e dibattito: il limite del ruolo degli intermediari quali custodi e insieme soggetti attivi nell'ecosistema dell'informazione. Anche perché cancellazione di informazioni e conservazione di informazioni, dunque oblio (in senso atecnico) e memoria, sono i due grandi opposti che plasmano la conoscenza delle società umane e la parabola individuale di ciascuno.

¹ <https://www.theguardian.com/technology/2021/may/27/facebook-lifts-ban-on-posts-claiming-covid-19-was-man-made>

L'EVOLUZIONE DELLE MISURE DI SICUREZZA QUALE FATTORE DI PROTEZIONE DEI DATI. UN CASO CONCRETO

Pierangelo Felici

Abstract: Tra le novità di maggior portata introdotte dal Regolamento Generale sulla Protezione dei Dati, l'onere, per il Titolare o il Responsabile del trattamento, di adottare misure di sicurezza adeguate. E quindi di evolverle nel tempo, seguendo la mutazione del contesto e rispondendo alla comparsa di nuovi rischi. Cosa succede quindi quando nasce un potenziale problema che possa rappresentare un rischio di violazione? Illustriamo un caso concreto che ha coinvolto molti soggetti, e che ha rappresentato un esempio della necessaria prevalenza della disciplina protezione dei dati rispetto a valutazioni diverse.

Among the most important innovations introduced by the General Data Protection Regulation, the obligation for the Data Controller or the Data Processor to adopt adequate security measures. And therefore to evolve them over time, following the mutation of the context and to respond to the emergence of new risks. So what happens when a potential problem that could pose a risk of infringement arises? We illustrate a concrete case that involved many subjects, and which represented an example of the necessary prevalence of the data protection discipline with respect to different assessments.

Parole chiave: misure di sicurezza, protezione dei dati, GDPR, ACN, adeguatezza

Sommario: 1. Introduzione – 2. Le Misure di sicurezza che evolvono – 3. Un esempio reale

1. Introduzione

Da quasi cinque anni, come è noto, è divenuto applicabile il Regolamento (UE) 679/2016 - General Data Protection Regulation - che ha cambiato diversi aspetti chiave nella tutela delle persone riguardo il trattamento, la protezione e la libera circolazione dei dati personali. La genesi sovranazionale della norma, in particolare, ha costretto i Titolari italiani a comprendere nuovi concetti e applicare modalità operative cui eravamo poco abituati, che spostano l'attenzione dalla esatta esecuzione di quanto puntualmente prescritto dal Legislatore alla cosiddetta "responsabilizzazione" di ciascun Titolare, che ha la libertà, ma di conseguenza l'onere e la responsabi-

lità, di effettuare le scelte di trattamento e di protezione dei dati più indicate per la propria organizzazione.

Uno degli ambiti più impattati da questo cambio di prospettiva è certamente quello delle misure di sicurezza connesse al trattamento di dati personali. Siamo infatti passati dalle “Misure minime di sicurezza”, un’elencazione precisa dei requisiti di protezione necessari e imposti per ciascuna categoria di dati personali, che era descritta nell’ *Allegato B* del D. Lgs. 196/2003, all’eliminazione del concetto stesso di “misure minime” a favore di quello di “misure adeguate”.

L’art. 32 del GDPR, al comma 1, infatti prescrive che

*“1. Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio(...)”*

La responsabilità di dover individuare le misure di sicurezza più adeguate diventa quindi attività del Titolare del trattamento, lasciando quindi all’Autorità di controllo la possibilità di verifica *ex post* e di eventuali interventi prescrittivi o sanzionatori.

Il Regolamento, poi, offre qualche indicazione su quali siano i parametri da considerare per poter valutare come adeguate le misure di sicurezza adottate o da adottare. E in particolare, le misure di sicurezza devono essere approntate tenendo conto dei seguenti criteri:

1. Lo stato dell’arte, e quindi lo standard di settore;
2. I costi di attuazione delle misure di sicurezza (e tenendo anche conto che tali misure andranno spesso a tutelare anche dati non personali, quindi devono essere valutate anche come un costo di investimento dell’organizzazione per la protezione dei propri asset, e non solo un mero obbligo);
3. La natura, l’oggetto, il contesto e le finalità del trattamento;
4. Il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche.

2. Le Misure di sicurezza che evolvono

In sostanza, quindi, l’obbligo di adottare misure adeguate, potrebbe essere vista come un’**obbligazione di mezzi**, che dovranno essere siano ragionevolmente soddisfacenti tenuto conto delle conoscenze e delle prassi tempo per tempo vigenti.

Ne deriva, naturalmente, che le misure di sicurezza non sono e non possono più essere “statiche”, ma devono continuare ad evolvere nel tempo, seguendo e adattandosi all’evoluzione delle minacce e dei rischi, e dovranno tener conto della sostenibilità, anche economica, del miglioramento continuo prescritto ora dalla norma.

Il Titolare del trattamento non ha più la possibilità, come con le norme precedenti, di “adeguarsi” *una tantum* per poi disinteressarsi dei cambiamenti sino ad eventuali

evoluzioni imposte dal Legislatore o dalle Autorità di settore. Ma dovrà, invece, assicurarsi di migliorare e adottare le misure di sicurezza che, sulla base dei principi prima richiamati, rappresenteranno lo “stato dell’arte” attuale, in ogni momento.

Cosa succede, quindi, quando un cambiamento di contesto, anche non voluto, o addirittura subito dal Titolare, varia le condizioni di rischio?

Il Regolamento GDPR, come si diceva, pone l’accento sulla cosiddetta “*accountability*” di Titolari e Responsabili, ossia, sull’adozione di comportamenti proattivi e sull’obbligo di dimostrare la concreta adozione di misure finalizzate ad abbattere il rischio. Nel momento in cui, quindi, diviene noto un evento, o un cambiamento di contesto, o l’esistenza di un fattore di rischio nuovo (o prima non considerato), diviene obbligo del Titolare rivalutare le misure di sicurezza adottate e, se necessario, riadeguarle. E questa evoluzione delle misure, se valutata necessaria, ha maggiore priorità rispetto a considerazioni diverse.

3. Un esempio reale

Un esempio concreto di tale necessità di rivalutazione e di priorità, che richiamiamo quale caso-scuola, si è avuto in molte organizzazioni italiane, e in particolare in molte Pubbliche Amministrazioni, nel corso dell’anno appena trascorso. Cerchiamo di descriverlo.

Come tutti sappiamo, il 24 febbraio 2022 è iniziata l’invasione, da parte delle forze militari della Federazione Russa, sul territorio dell’Ucraina. Al di là delle conseguenze economiche e geopolitiche, che non sono oggetto di questa trattazione, la guerra ha provocato un sensibile aumento dei tentativi di attacco informatico anche verso strutture del nostro paese, sia come azioni dirette (tentativi di accesso a sistemi volti all’accesso ai dati o alla interruzione di disponibilità, cosiddetti *Denial of Service*), sia come azioni indirette (tentativi di accesso a sistemi per prenderne il controllo in maniera trasparente, per poi essere usati quali punti di ulteriori attacchi nei confronti di terzi).

In questa situazione, il CSIRT-Italia, il Computer Security Incident Response Team istituito presso l’Agenzia per la Cybersicurezza Nazionale (ACN) aveva diffuso già il 28.02.2022 un Bollettino (BL01/220228/CSIRT-ITA) rilevando un incremento della frequenza delle attività di attacco anche verso strutture su territorio nazionale e consigliando di “Innalzare la postura difensiva in relazione alla situazione ucraina”, cioè aumentare il livello di controllo dei sistemi e servizi e adottare una serie di misure di natura tecnica e organizzativa volta a ridurre ulteriormente i rischi.

Già dai primissimi giorni post invasione, nei forum di confronto specialistico su cybersecurity e data protection, gli addetti ai lavori avevano iniziato a discutere sull’opportunità o meno, per le aziende e gli enti pubblici italiani ed UE, di continuare ad utilizzare l’antivirus Kaspersky, in quel momento piuttosto diffuso.

Il produttore, Kaspersky Lab, è infatti un’azienda russa ed era noto che collaborasse diret-

tamente nella gestione di alcuni sistemi informatici del Governo della Federazione Russa. Un sistema antivirus, a differenza di altri software, per sua stessa natura tecnica, ha ovviamente accesso *potenziale* in lettura e scrittura a qualunque risorsa e dato sul sistema. Ed è aggiornato/modificato direttamente dal produttore inviando e ricevendo dati in qualunque momento. Il 15.03.2022 l’Agenzia per la Cybersicurezza Nazionale ha poi diffuso un preallerta indicando che era: “opportuno considerare le implicazioni di sicurezza derivanti dall’utilizzo di tecnologie informatiche fornite da aziende legate alla Federazione Russa. (...) Alla luce di quanto sopra, l’Agenzia per la Cybersicurezza Nazionale, sentito il Nucleo per la cybersicurezza, raccomanda di **procedere urgentemente ad un’analisi del rischio derivante dalle soluzioni di sicurezza informatica utilizzate** e di considerare l’attuazione di opportune strategie di diversificazione.”

Ciò era di per sé già sufficiente a giustificare un’azione di rivalutazione del rischio ed eventuale sostituzione del software, proprio per le normative sulla protezione dei dati che **ci impongono di adottare misure di sicurezza – tempo per tempo – “adeguate al rischio”**.

Il software di cui si parla, in quel momento, era adottato ed usato correntemente da moltissime Pubbliche Amministrazioni italiane sia centrali (come diversi Ministeri o il Corpo della Guardia di Finanza, tra gli altri) sia locali (come molte ASL o moltissimi Comuni) che aveva conquistato grazie ad una politica commerciale, svolta anche tramite le Centrali di Acquisto Pubbliche, particolarmente efficace.

La decisione di procedere ad una sostituzione immediata, o comunque anticipata rispetto alla scadenza naturale dei contratti in essere, rappresentava una scelta molto forte e che generava anche dubbi di carattere normativo: alcuni si chiedevano, in particolare, se potesse una Pubblica Amministrazione ripagare (con altro fornitore) un prodotto/servizio che aveva in sostanza già pagato, in mancanza di un inadempimento esplicito e rilevabile da contestare al primo fornitore.

Per sciogliere i dubbi, vista l’urgenza che non consentiva differimenti significativi, è poi intervenuto il Governo Italiano, che con il *Decreto Legge 21.03.2022 n. 21* ha stabilito, tra l’altro, che “**Al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche** di cui all’articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, derivanti dal rischio che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Federazione Russa non siano in grado di fornire servizi e aggiornamenti ai propri prodotti appartenenti alle categorie individuate al comma 3, in conseguenza della crisi in Ucraina, **le medesime amministrazioni procedono tempestivamente alla diversificazione dei prodotti in uso.**” Lo stesso Decreto aveva quindi escluso che si potesse configurare il cosiddetto “danno erariale” per le azioni di cambio software in questione, ed era stato precisato che si potesse provvedere con le risorse vigenti. Cosa era successo, quindi? Che una **nuova situazione di rischio**, ragionevolmente non prevedibile prima, **aveva mutato le condizioni di contesto, e quindi i rischi per i diritti e le libertà degli interessati, derivanti dal trattamento informatizzato dei loro dati personali.**

Era quindi **onere di ogni Titolare e Responsabile rivalutare le misure di sicurezza adottate**, ed evolverle, anche sostenendo un costo, per riportarle a quello che l'art. 32 del Regolamento GDPR descrive come "lo stato dell'arte".

Ed è proprio questa, come si diceva, una delle novità di maggior portata introdotte dal Regolamento: al di là della compliance formale, **il Titolare del trattamento deve garantire una protezione dei dati che evolve seguendo la mutazione dei rischi sottesi al trattamento** e deve essere in grado di dimostrare *ex post* alle Autorità di controllo di aver fatto quanto ci si poteva ragionevolmente attendere.

L'accountability, quindi, rappresenta lo strumento per promuovere l'assunzione di decisioni e l'attuazione di meccanismi effettivi in un contesto in cui l'adempimento degli obblighi legali e la garanzia di un reale tentativo di protezione diventano indici virtuosi di tutela dei dati, e quindi dei diritti delle persone fisiche.

INTERRUZIONE VOLONTARIA DI GRAVIDANZA E PROTEZIONE DATI PERSONALI: L'ESEMPIO SPAGNOLO COME MODELLO PER NUOVE LINEE GUIDA DEL GARANTE DELLA PRIVACY?

Maria Angela Pisanu

Abstract: Il Regolamento n° 679/2016 ha introdotto nel nostro Paese alcuni elementi dalla portata rivoluzionaria. Si tratta di novità che dovrebbero incidere profondamente su una serie di prassi ormai consolidate in diversi ambiti, come nel caso del cd. "protocollo IVG" che riguarda la scelta di non portare a termine una gravidanza, percorso tutelato dalla Legge n° 194/1978. Ebbene, fin dal momento della sua entrata in vigore, la legge italiana non è mai stata modificata. A quarantacinque anni esatti dalla sua promulgazione, sarebbe quanto mai necessaria una rilettura "multi livellare" e "integrata", anche con il RGPD e il Codice della Privacy, per permetterle di acquisire nuove potenzialità come parte attiva di un cambiamento socioculturale orientato alla parità di genere. Invece il nostro Paese continua a rimanere "al palo" su una tematica così sensibile, decisamente arretrato rispetto ad altri Paesi europei, come il caso spagnolo, con il quale si propone un raffronto diretto dal punto di vista normativo e procedurale.

The General Data Protection Regulation No. 679/2016 has introduced in our country some revolutionary elements. These are changes that should profoundly affect a series of consolidated practices in various areas, as in the case of the so-called 'IVG protocol', concerning the voluntary termination of pregnancy, regulated in Italy by Law No. 194/1978.

Well, since its adoption, the Italian law has never been amended. Forty-five years after its promulgation, a 'multi-level' and 'integrated' reinterpretation, that would consider both the GDPR and the Privacy Code, would be more necessary than ever, aiming at driving a socio-cultural/gender-equality change.

On the contrary, our country continues to neglect such a sensitive issue, while other countries as Spain, whose case is discussed here, offers interesting points of direct comparison from both a regulatory and procedural point of view.

Parole chiave: Legge n° 194/1978, IVG, dati personali, pseudonimizzazione, anonimizzazione, accountability, cimitero dei feti, Garante della Privacy, Istituto Superiore di Sanità

Sommario: 1. Introduzione – 2. Spagna e Italia a confronto – 3. Il caso del *cimitero dei feti* di Roma Capitale – 4. Conclusioni

1. Introduzione

La scelta di non portare a termine una gravidanza, in Italia, è tutelata dalla **Legge n° 194/1978**¹.

Fin dal momento della sua entrata in vigore, abbiamo sempre sentito parlare di “protocollo IVG”² come di una procedura eseguita in “forma anonima”.

Questa legge nasce in un contesto storico completamente diverso da quello attuale, ma nell’esaminare tutte le possibili soluzioni alternative all’IVG, il legislatore introduce all’Art. 5 un concetto che, oggi, deve suscitare curiosità e desiderio di approfondimento per tutti coloro che studiano la materia della protezione dei dati personali.

L’Art. 5 sancisce prima di tutto un diritto potestativo esclusivo della paziente: “[...] *esaminare con la donna e con il padre del concepito, **ove la donna lo consenta***”. A seguire, specifica immediatamente che il protocollo avviene “[...] *nel rispetto della dignità e della **riservatezza** della donna e della persona indicata come padre del concepito [...]*”. Considerando il fatto che la riservatezza, così come la concepiamo ai giorni nostri, è uno dei parametri fondamentali da assicurare quando si parla di protezione dei dati personali, il richiamo alla normativa privacy viene quasi automatico.

Il **Regolamento n° 679/2016** (da ora in poi indicato come RGPD), con la sua portata rivoluzionaria, introduce diverse importanti novità quali, per citarne solo alcune, l’approccio basato sul rischio dei trattamenti e il principio di *accountability*, tradotto in italiano con il termine *responsabilizzazione*.

Questa nuova visione impone al Titolare del trattamento l’obbligo di dimostrare la conformità alla volontà del legislatore garantendo la protezione dei dati attraverso la scelta di misure tecniche e organizzative adeguate, atte a prevenire quanto più possibile i rischi per i diritti e le libertà dell’interessato.

Tra queste misure vi è certamente la **pseudonimizzazione**.

L’Art. 4, par. 5 del RGPD definisce la pseudonimizzazione come il “*trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*”.

In sintesi, il dato personale sostituito è da uno “pseudonimo” che viene utilizzato per tutta la durata del trattamento, garantendo appunto il parametro della riservatezza. Diversa è invece la pratica dell’anonimizzazione.

Confondere pseudonimizzazione e anonimizzazione dei dati è un errore molto diffuso³. Nelle definizioni che troviamo all’Art. 4 del RGPD non vi è una voce specifica

¹ Legge 22 maggio 1978, n. 194, Norme per la tutela sociale della maternità e sull’interruzione volontaria della gravidanza

² Acronimo di “interruzione volontaria di gravidanza”

³ Cfr. <https://www.cybersecurity360.it/legal/privacy-dati-personali/pseudonimizzazione-e-anonimizzazione-dei-dati-differenze-tecniche-e-applicative/>

per il concetto di “dato anonimo” o “informazione anonima”, ma la si può efficacemente desumere dal *Considerando 26* che spiega come “**i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime**, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l’identificazione dell’interessato”.

Fatta questa doverosa premessa, la domanda fondamentale da porsi in relazione alla pratica in “forma anonima” dell’IVG è: si può effettivamente parlare di anonimizzazione dei dati?

Un’analisi superficiale sembrerebbe portarci fuori dall’ambito del RGPD, ma in realtà non è così. È fondamentale affrontare sempre la questione della protezione dati almeno da due angolazioni distinte: il RGPD e la normativa nazionale di riferimento, vale a dire il **D. Lgs. n° 196/2003** (cosiddetto Codice della Privacy, da ora in poi indicato come Codice), ora novellato dal **D. Lgs. n° 101/2018**.

Questo perché proprio il RGPD, che all’Art. 9, par. 1 vieta espressamente il trattamento di dati relativi allo stato di salute, salvo non ricorrano particolari condizioni, al par. 4 del medesimo articolo introduce una clausola di specificazione che lascia ampio margine decisionale al legislatore interno (nello specifico, in questa sede opereremo un confronto con l’ordinamento spagnolo) proprio in merito al trattamento dei dati sanitari del soggetto interessato.

La nostra analisi non può pertanto prescindere da un’attenta lettura anche della normativa nazionale. Le strutture autorizzate, come ospedali pubblici e cliniche convenzionate, praticano la IVG gratuitamente e hanno l’obbligo di conformarsi alla normativa europea e nazionale in materia di protezione dati. L’Art. 2 *septies*, comma 8 del Codice, stabilisce che i dati personali delle pazienti che effettuano **qualunque tipo di prestazione sanitaria** non possono essere resi pubblici o divulgati, né tantomeno menzionati in alcun tipo di relazione⁴. Questo vale a maggior ragione se si parla di una pratica delicata come la IVG, tutelata da una legge *ad hoc*.

⁴ I dati relativi allo stato di salute ricevono una tutela anche in ambito penalistico. Il Codice, all’Art. 167 comma 2, stabilisce “Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all’interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 *sexies* e 2 *octies*, o delle misure di garanzia di cui all’articolo 2 *septies* ovvero operando in violazione delle misure adottate ai sensi dell’articolo 2 *quinqüiesdecies* arreca nocumento all’interessato, è punito con la reclusione da uno a tre anni”. La stessa Legge 194/1978 faceva già un riferimento alle ripercussioni penali all’Art. 21, stabilendo che “Chiunque, fuori dei casi previsti dall’articolo 326 del codice penale, essendone venuto a conoscenza per ragioni di professione o di ufficio, rivela l’identità - o comunque divulga notizie idonee a rivelarla - di chi ha fatto ricorso alle procedure o agli interventi previsti dalla presente legge, è punito a norma dell’articolo 622 del codice penale”. Questo articolo va però visto in un’ottica differente da quella della protezione dati, dato anche il contesto storico e temporale differente, poiché si riferisce alla violazione del segreto d’ufficio e professionale. Oggi, il RGPD opera più volte un netto richiamo al segreto professionale, come per esempio all’Art. 9 par. 3, dove è esplicitato che “I dati personali di cui al par. 1 possono essere trattati per le finalità di cui al par. 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell’Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch’essa soggetta all’obbligo di segretezza conformemente al diritto dell’Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti”.

2. Spagna e Italia a confronto

Avendo deciso di affrontare il tema attraverso una comparazione tra la normativa italiana e quella spagnola, è certamente interessante osservare lo spazio che quest'ultima dedica ai concetti di pseudonimizzazione e anonimizzazione dei dati personali. La **Ley Organica n° 2/2010**, all'Art. 21.1, stabilisce che *“i dati identificativi delle pazienti alle quali viene effettivamente erogata la prestazione, saranno soggetti a codificazione e separati dai dati clinici relativi all'interruzione volontaria della gravidanza”*⁵.

Successivamente, l'Art. 23.1, sancisce che *“la documentazione clinica può essere conservata in presenza di motivi epidemiologici, di ricerca o di organizzazione e funzionamento del sistema sanitario nazionale, nel qual caso tutti i dati identificativi della paziente e il codice che sarebbero stati assegnati saranno cancellati [...]”*⁶. Non ci troviamo ancora nell'ambito di applicazione temporale del RGPD. La Ley Organica spagnola, dal punto di vista della protezione dati, è però in linea con i dettami della **Direttiva n° 46/95**, trasposta nell'ordinamento interno spagnolo con la **Ley Organica n° 15/1999**.

Nel trattamento dei dati personali esiste una netta distinzione tra la fase IVG, che potremmo definire operativa, e la successiva fase di conservazione degli stessi dati riferiti alla pratica.

È evidente che, se nella prima fase si procede attraverso la pseudonimizzazione, la normativa spagnola prescrive successivamente la totale anonimizzazione in caso di conservazione *“per motivi epidemiologici, di ricerca o di organizzazione e funzionamento del sistema sanitario nazionale”*.

Pertanto, il concetto di procedura IVG *“in anonimato”* non deve trarre in inganno. Il concetto di *“anonimato”*, è legato più all'utilizzo del termine nella sua accezione di uso comune, poiché risulterebbe estremamente difficoltoso per una struttura sanitaria procedere senza avere a disposizione quantomeno i dati personali fondamentali per attivare il protocollo medico in modo sicuro.

Garantendo però la totale anonimizzazione dei dati in un momento successivo, possiamo affermare che *“l'evento IVG”*, pur essendo conservato all'interno degli archivi della struttura sanitaria, non può più in alcun modo essere ricondotto a un soggetto identificabile e, anche nel caso in cui non si proceda con la conservazione dei dati per le finalità precedentemente citate, la normativa spagnola obbliga il personale sanitario, trascorsi i cinque anni dalle dimissioni della paziente, a operare d'ufficio la cancellazione dei dati.

⁵ Art. 21.1, Ley Organica 2/2010 *“los datos identificativos de las pacientes a las que efectivamente se les realice la prestación serán objeto de codificación y separados de los datos de carácter clínico asistencial relacionados con la interrupción voluntaria del embarazo.”*

⁶ Art. 23.1, Ley Organica 2/2010: *“la documentación clínica podrá conservarse cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud, en cuyo caso se procederá a la cancelación de todos los datos identificativos de la paciente y del código que se le hubiera asignado [...]”*

Con la Ley Organica n° 2/2010, attuata con la riforma Zapatero che, di fatto, modifica la normativa originaria del 1985 - che si limitava a rettificare l'Art. 417 bis del Código Penal⁷- la Spagna introduce la tutela dei dati personali tra i diritti fondamentali della paziente che sceglie di sottoporsi alla pratica di IVG. È interessante notare come la formulazione degli Artt. da 20 a 23 della normativa del 2010 non sia poi così distante da quelli che saranno i principi sanciti dal RGPD nel 2016.

A differenza della sua omologa spagnola, la legge italiana non è mai stata modificata dal momento in cui è entrata in vigore nel 1978, né il legislatore ha ritenuto opportuno di dover inserire al suo interno il richiamo, per esempio, alla redazione di un decreto ministeriale o un regolamento governativo di esecuzione che ne facilitassero la corretta applicazione.

Le strutture sanitarie hanno sempre operato basandosi unicamente sulla legge ordinaria che, dal punto di vista della riservatezza, richiama solo l'obbligo del segreto d'ufficio e del segreto professionale. Ma le varie normative su riservatezza, segreto professionale e segretezza non hanno mai realmente tutelato in modo adeguato i singoli dalla raccolta e dall'utilizzo abusivo dei dati personali.

«La Legge n° 194 non ha richiami specifici alla privacy e protezione dati», spiega il Prof. Giambenedetto Melis, già direttore della Clinica Ostetrica e Ginecologica dell'Università degli Studi di Cagliari e ora Responsabile del Centro S.O.M.A. per la Salute della Donna. **«In prima istanza vi era solo il riferimento al segreto professionale, cui poi è stata affiancata la Legge n° 675/1996, che è stata la prima legge sulla privacy entrata in vigore nel nostro Paese»**.

Nell'ambito operativo medico le normative vengono applicate *in toto* nelle varie fasi. Però ci sono situazioni, come quella relativa alla pratica IVG, che necessitano di maggiore approfondimento. Basti pensare alla richiesta inversa di una paziente che desidera, per esempio, partorire in totale anonimato: non esistono ancora normative specifiche che disciplinino tali fattispecie.

«Il Ministero della Salute» continua il Prof. Melis **«discute da diversi anni su quali possano essere, a livello nazionale, le metodiche standard affinché si riesca a realizzare una cartella clinica senza citare il nome della paziente e su come sia possibile risalire eventualmente in seguito, in casi assolutamente eccezionali, per esempio per motivi giudiziari, a tale dato personale. Per dovere di completezza, la discussione a livello formale riguarda solo il parto e non si è ancora arrivati a discutere dell'IVG. A livello sostanziale, comunque, nelle strutture sanitarie pubbliche, le situazioni del parto “in anonimato” e dell'IVG sono trattate in modo analogo»**.

Riassumendo, dal punto di vista strettamente inerente alla protezione dati, per “anonimato” si intende esclusivamente il fatto che i dati personali della paziente non

⁷ La modifica attuata rispetta pienamente quanto sancito durante la “Conferenza Mondiale sulle donne” tenutasi nel 1995 a Pechino, che ha riconosciuto come “i diritti umani delle donne includono il diritto ad avere il controllo e a decidere liberamente e responsabilmente sulla propria sessualità, compresa la salute sessuale e riproduttiva, senza pressione, discriminazione e violenza”.

possano essere diffusi all'esterno della struttura, come stabilito dall'Art. 2 *septies* comma 8 del Codice e vi è una tutela della riservatezza esclusivamente da un punto di vista logistico: alle pazienti vengono riservati ambienti non identificati o identificabili e stanze separate dal resto del reparto, per evitare che entrino in contatto con le puerpere, come stabilito anche dagli standard di sicurezza previsti nell'Accordo Stato-Regione del 16 dicembre 2010 sul riordino dei punti nascita.

Tecnicamente non si può assolutamente parlare di **anonimizzazione** dei dati personali.

Infine, a differenza di quanto avviene in Spagna, dove le strutture portano avanti il protocollo IVG ricorrendo alla **pseudonimizzazione**, in Italia i dati della cartella clinica sono addirittura **in chiaro**, visibili a tutti gli operatori autorizzati a entrare in contatto con il fascicolo e, spesso, anche a soggetti terzi non direttamente coinvolti nel protocollo.

Richiamando il principio di *accountability*, questa situazione procedurale consolidata determina un livello di rischio molto maggiore e una carenza dal punto di vista delle misure di sicurezza tecniche e organizzative atte a garantire il rispetto dei diritti e delle libertà della paziente, oltre al perdurare di una notevole distanza dai dettami attualmente prescritti dal RGPD.

3. Il caso del *cimitero* dei feti di Roma Capitale

Una buona legge è quella che rispetta la Costituzione e che viene interpretata e applicata seguendone i dettami. La Legge n° 194/1978 ha certamente subito i segni del tempo e si dimostra a tratti claudicante. Le prassi erranee si sono susseguite per oltre quarant'anni. L'ultima e più famosa è sicuramente la vicenda incresciosa del *cimitero dei feti* di Roma Capitale del 2020, episodio che ha visto **la sepoltura dei materiali abortivi con la dicitura in chiaro dei nomi delle madri**.

A due anni di distanza, il Tribunale di Roma ha archiviato il procedimento penale, stabilendo la non sussistenza del dolo né la lesione della privacy, ma solo una "prassi erronea dipesa da un contesto poco chiaro a livello di normativa".

Non possiamo a questo punto esimerci da una riflessione profonda.

È stata evidenziata una carenza normativa, carenza che ha portato all'identificazione dei feti mediante l'apposizione dei nomi delle donne sottoposte a IVG sulle croci, scelta che già di per sé pare stigmatizzare ancora di più la loro *colpa*.

«**La Procura**» ha commentato amaramente l'avvocata di *Differenza Donna* Ilaria Boriani «**nella richiesta di archiviazione, insieme all'Autorità Garante della privacy, accerta un trattamento illecito su dati sensibilissimi in tutta la filiera, a partire dalle aziende ospedaliere fino alla sepoltura e all'esposizione del nome. Tuttavia, ha ritenuto e ribadito in aula la non sussistenza dell'elemento soggettivo, cioè della consapevolezza della volontà di violare le norme, desunta anche da una normativa di difficile comprensione [...]. Infatti, la normativa a tutela della**

privacy è quanto di più difficile esista nel nostro ordinamento e non si può esercitare l'azione penale nei confronti delle persone indagate»⁸.

A caldo, verrebbe da storcere il naso e commentare che in Italia vige il principio “*ignorantia legis non excusat*”. Ma, parafrasando ironicamente Carlo Lucarelli, *questa è un'altra storia*.

La storia che interessa a noi, cittadini e cultori della protezione dati, è che in questa triste vicenda si è reso necessario l'impulso dell'Autorità Garante per spingere verso un'accelerazione e un immediato correttivo da parte del Comune di Roma per modificare il Regolamento di Polizia cimiteriale, nonché i protocolli riguardanti il trattamento dei dati personali. Perché, se è vero che i morti non hanno diritto alla protezione dei dati personali, per i vivi è tutt'altra questione.

L'Autorità, dopo l'apertura dell'istruttoria nel 2020, ha indicato apposite istruzioni operative atte a rimuovere la violazione e in previsione di nuovi futuri trattamenti, suggerendo a tale proposito l'utilizzo di un codice alfanumerico per l'identificazione del feto. Il ricorso alla pseudonimizzazione non fa altro che ripristinare la proporzionalità nei trattamenti, in ossequio al principio di minimizzazione, bilanciando così tutti gli interessi in gioco.

Anche se il giudice ha sentenziato la totale assenza di dolo, **l'illecita diffusione dei dati particolarmente sensibili e la violazione della riservatezza delle donne che hanno avuto accesso all'IVG resta comunque un fatto sostanzialmente incontrovertibile e per nulla etico**. La vicenda del “cimitero dei feti” e la sua conclusione, ci dimostra quanto il nostro Paese seguiti a restare incagliato a vecchi formalismi e ancora lontano dal principio di *accountability*.

4. Conclusioni

Se, da un lato, la Spagna si incammina sempre più rapidamente verso un totale riconoscimento del diritto a una libera vita sessuale, tanto da modificare nuovamente il Código Penal e qualificare come reato il tentativo di importunare o intimidire una donna che si reca in una struttura sanitaria per abortire⁹, **il nostro Paese continua a rimanere “al palo” su una tematica così sensibile**.

L'Italia non può fare altro che guardare da lontano il Paese iberico. Il contesto spagnolo, infatti, funge da innesco a un panorama apertissimo di riflessioni, favorendo molteplici punti di vista¹⁰. Con le ultime riforme targate 2022¹¹, diviene il pioniere,

⁸ Cfr. <https://www.open.online/2022/01/22/cimitero-feti-roma-inchiesta/>

⁹ Cfr. https://www.cortecostituzionale.it/documenti/segnalazioni_corrente/Segnalazioni_1650015672230.pdf

¹⁰ Per maggiori approfondimenti si rimanda a Marta León Alonso y María Candelaria Sgró Ruata, Córdoba [Argentina], *La reforma del aborto en España: perspectivas de un debate (re)emergente*, 2014

¹¹ Nel maggio 2022, il governo socialista presieduto da Pedro Sánchez ha approvato un disegno di legge che mira a portare l'interruzione volontaria di gravidanza nei centri pubblici, inserire dei punti fermi sull'obiezione di coscienza, consentire alle donne in fascia di età 16/17 anni di accedere all'IVE

uno dei più avanzati al mondo per quel che riguarda la tutela del diritto a una libera vita sessuale, all'aborto, ma anche e soprattutto alla tutela della protezione dati delle donne che vi si sottopongono.

Allo stato attuale, viceversa, non appare pensabile in Italia un ampliamento diretto della Legge n° 194/1978 tramite iter legislativo ordinario o abbreviato. Ma, in realtà, dal punto di vista del diritto alla protezione dei dati personali, non sarebbe neppure necessario. Si potrebbe ipotizzare invece una pronuncia congiunta tra la nostra Autorità di Controllo e l'Istituto Superiore di Sanità, con la conseguente emanazione di linee guida dedicate da inserire poi anche nel Sistema Nazionale per linee Guida (SNLG) del Ministero della Salute. Quest'atto formale non modificherebbe la normativa, ma la aiuterebbe a vivere di nuovo al passo coi tempi.

Osservandola oggi, a quarantacinque anni esatti dalla sua promulgazione, la Legge n° 194/1978 avrebbe solo bisogno di riconfermare il suo reale orientamento costituzionale. Una rilettura in quell'ottica "multilivello" e "integrata", anche con il RGPD e il Codice, potrebbe permetterle di acquisire nuove potenzialità come parte attiva di un cambiamento socioculturale orientato alla parità di genere.

Ringraziamenti:

- Prof. Massimo Farina, il mio mentore, per i preziosi insegnamenti e la grande passione che è riuscito a trasmettermi per la disciplina della protezione dati.
- Avv. Alessia Palladino, per la guida nella stesura iniziale di questo lavoro di ricerca.
- Avv. Andrea Lisi, per l'impulso a non abbandonare lo studio di una materia tanto affascinante quanto complessa e l'invito a dare il mio piccolo contributo alla *conoscenza*.
- Prof. Gian Benedetto Melis, per la consulenza su protocolli ospedalieri nazionali IVG.
- Dott.ssa Barbara Zedda, per la preziosa collaborazione nel reperimento e nella verifica delle fonti e per il supporto editing.
- Dott. Andrea Granitzio, per avermi trasmesso l'approccio *artistico* alle scienze giuridiche.
- Avv. Nicola Fabiano, per l'incoraggiamento a costruire la mia "coscienza etica".

(Interrupción Voluntaria del Embarazo) senza il consenso dei genitori, eliminare l'obbligo di ricevere informazioni sulla maternità ed eliminare i tre giorni di "periodo di riflessione", oltre che riconosce per la prima volta il diritto alla salute mestruale. La proposta è stata approvata dal Congresso a fine dicembre 2022 ed è opinione diffusa che entrerà in vigore prima della fine della legislatura.

Per ulteriori approfondimenti si rimanda a <https://www.elmundo.es/espana/2022/05/17/62835e82fc6c8329648b457a.html>, <https://www.lavanguardia.com/vida/junior-report/20220902/8495826/nuevalley-aborto-espana.html> e https://www.igualdad.gob.es/comunicacion/notasprensa/Documents/NdeP/NdeP_CMin_300822.pdf

Fonti normative, dottrina e bibliografia:

- EU 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 (regolamento generale sulla protezione dei dati)
- IT D. Lgs. n° 196/2003 recante il “Codice in materia di protezione dei dati personali” novellato dal D. Lgs. 101/2018 recante “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)”
- IT Legge n° 194/1978 Norme per la tutela sociale della maternità e sull’interruzione volontaria di gravidanza
- IT Accordo Stato-Regioni 12/2010 Percorso nascita
- ES Ley n° 16/2003, de cohesión y calidad del Sistema Nacional de Salud
- ES Ley Orgánica n° 15/1999, de Protección de Datos de Carácter Personal
- ES Ley Orgánica n° 3/2018 de Protección de Datos Personales y garantía de los derechos digitales
- ES Ley Orgánica n° 9/1985, de Reforma del artículo 417 bis del Código penal.
- ES Ley Orgánica n° 2/2010, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo
- IT <https://snlg.iss.it> Istituto Superiore di Sanità - Servizio Nazionale Linee Guida
- IT Douwe Korff - Marie Georges (con il contributo del Garante italiano per la protezione dei dati personali & dei Partner del progetto), T4DATA - Manuale per gli RPD, Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell’Unione Europea, (2019)
- IT Nicola Fabiano, GDPR&PRIVACY, Consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity, GoWare, 2019.
- IT Edoardo Limone, <https://www.cybersecurity360.it/legal/privacy-dati-personali/pseudonimizzazione-e-anonimizzazione-dei-dati-differenze-tecniche-e-applicative/>, 17/10/2019.
- IT <https://www.open.online/2022/01/22/cimitero-feti-roma-inchiesta/>, 22/01/2022.
- IT https://www.cortecostituzionale.it/documenti/segnalazioni_corrente/Segnalazioni_1650015672230.pdf, 15/04/2022
- ES: Marta León Alonso y María Candelaria Sgró Ruata, Córdoba [Argentina], *La reforma del aborto en España: perspectivas de un debate (re)emergente*, 2014
- ES <https://www.elmundo.es/espana/2022/05/17/62835e82fc6c8329648b457a.html>, 30/08/2022
- ES <https://www.lavanguardia.com/vida/junior-report/20220902/8495826/nueva-ley-aborto-espana.html>, 02/09/2022

I SISTEMI DI VIDEOSORVEGLIANZA IN AZIENDA: UN DELICATO BILANCIAMENTO FRA I TANTI DIRITTI IN GIOCO

Eleonora Mataloni

Abstract: La videosorveglianza in azienda costituisce un argomento spinoso sotto diversi profili. In Italia la materia è regolata da plurime fonti normative: dal Codice civile, al D.Lgs. n. 151 del 14 settembre del 2015, il cd. Jobs Act, che ha riformulato l'art. 4 dello Statuto dei Lavoratori, dal novellato D.Lgs. giugno 2003, n.196 (Codice in materia di protezione dei dati personali) alla normativa sovranazionale rappresentata dal Regolamento Europeo n. 679/16 (GDPR). Se i tempi di conservazione delle immagini e l'obbligo di dedicare informative ad hoc contenenti la regolamentazione di tale trattamento sono un aspetto prioritario che il datore di lavoro deve rispettivamente regolamentare e adottare nella propria azienda, un altro argomento di particolare importanza è rappresentato dal contemperare un bilanciamento fra il diritto di controllare che l'attività lavorativa dei dipendenti e il dovere di rispettare la loro riservatezza, dignità personale, la loro libertà di espressione e di comunicazione

Video surveillance in companies constitutes a thorny topic in several respects. In Italy, the matter is regulated by multiple regulatory sources: from the Civil Code to Legislative Decree No. 151 of Sept. 14, 2015, the so-called Jobs Act, which reformulated Article 4 of the Workers' Statute, from the revised Legislative Decree June 2003, No. 196 (Code on the Protection of Personal Data) to the supranational rules of the European Regulation No. 679/16 (GDPR). The retention time of images and the obligation to arrange ad hoc notices, which contain the regulation of such processing, are priority issues that employers have to, respectively, regulate and adopt in their companies. Moreover, the other issue of preeminent importance is the balancing of the right to control employees' activity along with the duty to respect their confidentiality, personal dignity, freedom of expression and communication.

Parole chiave: videosorveglianza, controlli a distanza del lavoratore, Regolamento - GDPR.

Sommario: 1. Introduzione - 2. Videosorveglianza e protezione de dati: la normativa sovranazionale e di settore - 3. I controlli a distanza del lavoratore e la conformità alle prescrizioni del Reg. UE 679/16 - 4. I provvedimenti del Garante per la protezione dei dati personali - 5. La cd. videosorveglianza “domestica”: brevi cenni

1. Introduzione

Negli ultimi anni abbiamo assistito ad un vero e proprio *exploit* della videosorveglianza. Il settore è, infatti, interessato da una sempre maggiore ed inarrestabile evoluzione tecnologica, causata anche dalla necessità di rispondere in maniera puntuale ed esauriente alle più accentuate e sentite richieste di protezione e sicurezza che pervengono sia da soggetti qualificati (aziende, Enti) sia da semplici cittadini. In questo contesto si situa il provvedimento sulla sicurezza urbana (D.L. 20 febbraio 2017, n. 14, convertito in legge 18 aprile 2017, n. 48, pubblicata in G.U. n. 93, serie generale, del 21 aprile 2017) c.d. “Decreto Minniti”, che ha ampliato l'utilizzo della videosorveglianza, incentivando gli Enti pubblici ad investire in sistemi di videosorveglianza “intelligente”.

Nel settore privato, a circa cinque anni dall'entrata in vigore del GDPR, le ultime statistiche indicano che in linea generale solo un'azienda su quattro si è adeguata, e si tratta perlopiù di grandi realtà e multinazionali, mentre le cd. PMI e le microimprese faticano ancora a conformarsi alla nuova normativa sulla protezione dei dati personali. I soggetti avrebbero dovuto attivarsi per essere in regola entro il 25 maggio 2018 anche sotto il profilo del trattamento dei dati acquisiti mediante un sistema di videosorveglianza.

2. Videosorveglianza e protezione dei dati: la normativa sovranazionale e di settore

Privacy e videosorveglianza: l'argomento è di particolare attualità se solo si considera che da un'indagine svolta lo scorso giugno 2022 ne emerge un quadro abbastanza preoccupante su quello che è lo stato dell'arte italiano in tema di applicazione delle regole sulla videosorveglianza.

Ed invero, su un campione di circa 2.000 individui, nel 92% dei casi i sistemi di videosorveglianza non risultano rispettare il GDPR.

Secondo tale rapporto, solo l'8% degli intervistati è entrato in un esercizio pubblico dotato di un sistema audiovisivo trovandovi un'informativa ridotta rispettosa dei requisiti richiesti dalle normative vigenti e delle indicazioni del Garante.

Nel 38% dei casi non c'è alcun cartello che avvisi gli avventori della presenza delle telecamere, mentre nei restanti casi, benché presente, il cartello risulterebbe non compilato con le informazioni necessarie oppure corredato da riferimenti normativi obsoleti o sbagliati mentre nel 38% dei casi non c'è alcun cartello che avvisi gli avventori della presenza delle telecamere, mentre nei restanti casi, benché presente, il cartello risulterebbe non compilato con le informazioni necessarie oppure corredato da riferimenti normativi obsoleti o sbagliati.

L'esigenza di sicurezza deve però coordinarsi con la doverosa tutela del diritto alla

riservatezza delle persone, per cui l'utilizzo delle nuove tecnologie dovrà essere effettuato alla luce della normativa vigente, che si è arricchita del recente 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 essi, che abroga la Direttiva 95/46/CE (GUUE 4 maggio 2016, L 119/1) entrato in vigore il 25 maggio 2018.

Ed invero, la materia della videosorveglianza si intreccia con la disciplina prevista dallo **Statuto dei lavoratori** (legge n. 300/1970) e, in particolare, con le norme contenute nel Titolo I, rubricato «Della libertà e dignità del lavoratore».

L'articolo 4 della L. 300/1970 è il cuore della disciplina relativa ai controlli a distanza dei lavoratori.

Il 24 settembre è entrato in vigore il D.Lgs. n. 151/2015, attuativo di una delle deleghe contenute nel c.d. Jobs Act, che modifica e riformula l'articolo 4 dello Statuto dei lavoratori in materia di videosorveglianza, adeguando le disposizioni e le procedure preesistenti alle innovazioni tecnologiche e alla loro introduzione nei contesti aziendali. L'avvento del D.lgs. 81/2015 (*Jobs Act*) ha impattato sulla disciplina dei controlli a distanza, andando a modificare lo stesso articolo 4.

Analizziamo il testo dell'articolo prima e dopo il *Jobs Act*.

Art. 4, L. 300/1970 **prima del D.lgs. 81/2015** (*Jobs Act*):

«È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti»

Art. 4, L. 300/1970 **dopo il Dlgs. 81/2015** (*Jobs Act*):

*«Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori **possono essere impiegati** esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e **per la tutela del patrimonio aziendale** e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali.*

*La disposizione di cui al comma 1 non si applica agli **strumenti utilizzati dal la-***

avoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

Il Jobs Act si è proposto quindi, relativamente al tema dei controlli a distanza del lavoratore, di riformare l'articolo 4 dello Statuto dei Lavoratori introducendo alcuni aspetti innovativi:

Primo elemento fondamentale della proposta di riforma: viene inserita fra le finalità perseguite la “tutela del patrimonio aziendale”, non presente nella precedente dizione normativa;

Secondo elemento fondamentale della proposta di riforma: vengono esclusi dal perimetro dell'accordo sindacale i sistemi di controllo accessi (dovendosi intendere gli accessi fisici ai locali e, interpretando in via estensiva la parola “accesso”, gli accessi logici ai sistemi informatici) e di controllo presenze (superando così la Sentenza della Corte di Cassazione n° 15892/2007).

Restano in perimetro di accordo sindacale tutti i sistemi di controllo che non siano nativi dello strumento messo nella disponibilità del lavoratore o che comunque raccolgano informazioni ulteriori rispetto al mero “accesso” ai locali fisici o ai sistemi informatici (content filtering, data loss prevention, MAM per device mobili, servizi di geolocalizzazione strumenti e di effettuazione dei controlli) nel rispetto di quanto disposto dalla normativa in tema di protezione di dati personali.

Terzo elemento essenziale della proposta di riforma: per trattare legittimamente le informazioni raccolte occorre rispettare l'obbligo informativo di cui all'art. 13 GDPR nonché quanto previsto dal Provvedimento dell'Autorità Garante per la protezione dei dati personali del primo marzo 2007 (adozione di un disciplinare interno redatto in forma non generica).

«Le informazioni raccolte ai sensi dei commi 1 e 2 (art. 4 Jobs act) sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.»

In sostanza il Jobs Act ha introdotto un regime diverso a seconda del tipo di strumento utilizzato prevedendo che:

- per gli impianti audiovisivi e gli altri strumenti che consentono il controllo a distanza del lavoratore permane il divieto di installazione salvo esigenze specifiche e l'accordo sindacale/l'autorizzazione dell'INL;
- per gli strumenti di lavoro e per gli strumenti di registrazione di accessi e presenze non opera alcun divieto e alcun obbligo di accordo sindacale o di autorizzazione dell'INL;
- sia per i primi che per i secondi il datore ha l'obbligo di fornire ai dipendenti adeguata informazione circa le modalità d'uso degli strumenti e di effettuazione dei controlli nonché l'obbligo di rispettare la normativa sulla privacy nella raccolta e nel trattamento dei dati

3. I controlli a distanza del lavoratore e la conformità alle prescrizioni del Reg. UE 679/16

La possibilità per il datore di lavoro di adottare controlli a distanza nei confronti dei lavoratori, deve fondarsi sui principi normativi appena illustrati per non minare il delicato equilibrio fra garantire la tutela della dignità del lavoratore e il proprio diritto alla tutela dei beni aziendali.

Fra i principi in questione si ricordano quello di necessità in base al quale il controllo deve risultare necessario o indispensabile rispetto ad uno scopo determinato ed avere il carattere dell'eccezionalità, dovendo essere limitato nel tempo e nell'oggetto, mirato e mai massivo.

Ancora, il datore di lavoro deve rispettare il principio di finalità, rispetto al quale il controllo deve essere finalizzato a garantire la sicurezza o la continuità aziendale.

Infine, il sistema di videosorveglianza deve sottostare al principio di proporzionalità, in virtù del quale detto sistema deve essere caratterizzato da forme di controllo non eccedenti rispetto alla finalità di poter controllare l'attività lavorativa.

Con riferimento a tale tematica, di fondamentale importanza risulta la circostanza che il datore di lavoro deve essere in grado di individuare, sia nell'informativa dedicata ai propri dipendenti, sia nell'informativa cd. "estesa" sulla videosorveglianza da esporre in azienda (in luogo visibile a tutti gli interessati al trattamento, tra cui gli stessi clienti e fornitori) la corretta base giuridica del trattamento.

Quest'ultima può infatti essere rappresentata, sulla scorta dell'art. 6 GDPR nelle seguenti condizioni di liceità:

- adempimento di obblighi derivanti da un contratto di lavoro;
- adempimento di obbligazioni previste dalla legge;
- interesse legittimo del datore di lavoro.

Tra le norme dettate dal GDPR che vengono in rilievo in tema di sistema di videosorveglianza aziendale e controlli dei lavoratori, non si può non fare riferimento all'art. 88 GDPR in base al quale gli Stati possono emanare regole particolari atte a garantire la protezione dei diritti e delle libertà dei dipendenti durante i trattamenti dei dati nel contesto del rapporto di lavoro.

Questo può avvenire tramite accordi collettivi o disposizioni legislative. Il GDPR prevede, quindi, che le attività di controllo del lavoratore siano svolte in un contesto di trasparenza e di adeguata protezione dei dati personali.

A titolo esemplificativo, il controllo del datore di lavoro può avvenire a partire dalla valutazione dei candidati in sede di assunzione, oppure in occasione delle verifiche svolte in ambito di salute e sicurezza dell'ambiente di lavoro, o ancora in caso di eventuale recesso del lavoratore da rapporto di lavoro.

In tutti questi ambiti, è necessario che il datore di lavoro abbia adottato gli strumenti idonei a garantire il rispetto delle norme che regolano l'installazione di un impianto di videosorveglianza.

È necessario inoltre tenere conto del tipo di strumento utilizzato per effettuare il controllo del lavoratore (es. videosorveglianza, PC, smartphone). L'installazione di impianti audiovisivi e altri strumenti dai quali deriva anche la possibilità di controllo a distanza dell'attività dei lavoratori è di norma vietata, ad eccezione che il datore di lavoro provi la finalità del trattamento rappresentata da esigenze organizzative e produttive, di sicurezza del lavoro e tutela del patrimonio aziendale oppure sia stato stipulato un preventivo accordo sindacale (o, in mancanza, autorizzazione della Direzione territoriale del lavoro).

Da sottolineare come l'accordo sindacale o la detta autorizzazione devono sempre precedere l'installazione dell'impianto, non solo la messa in funzione come ben ha ricordato la Suprema Corte, sez. penale, con la sentenza n. 4331 del 2014.

Tra le novità della riforma introdotta con il Job Act, è opportuno ricordare ulteriormente quella introdotta dal secondo comma dell'articolo 4 dello Statuto dei Lavoratori, così come riformato, il quale prevede che le garanzie non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (es. smartphone, tablet, personal computer), e agli strumenti di registrazione degli accessi e delle presenze. In tali casi l'installazione non richiede alcun accordo sindacale, sebbene il Ministero del Lavoro abbia stabilito che nel momento in cui lo strumento viene modificato, consentendo ad esempio, la localizzazione del lavoratore, non è più possibile annoverarlo in tale categoria.

Ancora, il comma 3 stabilisce che le informazioni raccolte tramite gli strumenti di cui al comma 1 e 2, sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che al lavoratore sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.

Merita infine un breve cenno il tema della geolocalizzazione dei veicoli, i cui sistemi di monitoraggio ben possono essere posti per tutelare la sicurezza dei veicoli e dei lavoratori

Tale trattamento assume invece i caratteri della illecita è qualora i veicoli aziendali possano essere usati anche per finalità private.

Sul punto, il Garante ha avuto modo di affermare che il dipendente deve non solo essere informato che il datore di lavoro stia ponendo in essere un simile monitoraggio, ma deve anche essere messo nelle condizioni di poter disattivare tale sistema di controllo nel momento in cui svolge un'attività di natura personale con l'auto.

Tra gli obblighi cui il datore di lavoro è soggetto per essere *compliance* in tale situazione è quello di predisporre un'informativa all'interno del veicolo, ben leggibile, che ricordi al dipendente l'esistenza del sistema di monitoraggio e come poter interrompere tale trattamento.

4. I provvedimenti del Garante per la protezione dei dati personali

Rispetto all'importanza e alla delicatezza del tema in esame, Il Garante ha avuto modo, negli anni, pronunciare numerosi provvedimenti generali in tema di videosorveglianza, tra cui, solo per ricordare quelli principali:

- Provv. 29 novembre 2000 «Il decalogo delle regole per non violare la privacy» - [doc. web n. 31019];
- Provv. Generale 29 aprile 2004 - [doc. web n. 1003482];
- Provv. Generale 8 aprile 2010 - [doc. web n. 1712680];
- Circolare INL n. 5/2018 del 19 febbraio 2018

Circa le finalità, il Garante precisa più volte che il trattamento di dati personali attraverso i sistemi di videosorveglianza è lecito quando:

- È fondato su uno dei presupposti di liceità che il Regolamento 679/16 e il Codice in materia di protezione prevede espressamente in capo a soggetti pubblici e privati;
- È fondato sul principio di finalità. I sistemi di videosorveglianza in azienda hanno la finalità di protezione e incolumità dei dipendenti e di eventuali terzi, di protezione della proprietà e del patrimonio aziendale, di acquisizione delle prove nell'ambito dei c.d. controlli difensivi;
- È rispettato il principio di necessità: ciò comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (art. 5 GDPR - ex art. 3 del Codice);
- È rispettato il principio di proporzionalità tra i mezzi impiegati e i fini perseguiti per garantire un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 5 GDPR - ex art. 11, comma 1, lett. d) del Codice).

In altre parole: gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente ritenute insufficienti o inattuabili.

Gli interessati devono essere sempre informati quando stanno per accedere ad una zona videosorvegliata. Tale importante principio è stato oggetto di una sentenza della Corte di Cassazione (sez. II civ., sentenza 19 aprile - 5 luglio 2016, n. 13663) a mente della quale *«L'installazione di un impianto di videosorveglianza all'interno di un esercizio commerciale, costituendo trattamento di dati personali, deve formare oggetto di previa informativa, ex art. 13 del D.Lgs. n. 196 del 2003, resa ai soggetti interessati prima che facciano accesso nell'area videosorvegliata, mediante supporto da collocare perciò fuori del raggio d'azione delle telecamere che consentono la raccolta delle immagini delle persone e danno così inizio al trattamento stesso»*

Anche lo stesso Regolamento europeo n.679/16 impone poi l'obbligo di segnalare il sistema di videosorveglianza: l'interessato deve essere previamente informato che sta per accedere in una zona sorvegliata, per cui l'informativa deve essere colloca-

ta prima del raggio d'azione della telecamera ed essere chiaramente visibile agli interessati, in ogni area monitorata dalle telecamere.

Nello specifico, il supporto con l'informativa non solo deve essere collocato prima del raggio di azione della telecamera ma anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

Ancora, l'informativa deve avere un formato ed un posizionamento tale da essere chiaramente visibile, in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

Può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati, al fine di informare se le immagini siano solo visionate o anche registrate.

Il cartello che identifica un'area videosorvegliata deve riportare, ancora, gli estremi identificativi del Titolare del trattamento (la società e/o la ditta o anche il singolo professionista) e lo scopo dell'attività di monitoraggio mediante la videoripresa.

Il sistema di videosorveglianza impiegato deve essere infine programmato in modo da operare al momento prefissato l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto da ogni supporto, anche mediante sovra registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

In presenza di impianti basati su tecnologia non digitale o comunque non dotati di capacità di elaborazione tali da consentire la realizzazione di meccanismi automatici di expiring dei dati registrati, la cancellazione delle immagini dovrà comunque essere effettuata nel più breve tempo possibile per l'esecuzione materiale delle operazioni dalla fine del periodo di conservazione fissato dal titolare.

Il Garante individua anche precise finalità, alle quali è preordinato un impianto di videosorveglianza, ossia:

- Protezione e sicurezza del personale;
- Protezione e sicurezza dei clienti (o terzi);
- Protezione della proprietà o del patrimonio aziendale;
- Acquisizione di prove (c.d. controlli difensivi).

Queste finalità devono bilanciarsi con il diritto alla riservatezza e alla dignità delle persone, con particolare riguardo ai lavoratori e alla luce dello Statuto dei lavoratori (legge n. 300/1970).

Il Titolare (o il Responsabile) devono designare per iscritto tutte le persone fisiche incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini.

Occorre individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

La nomina dei soggetti autorizzati è un profilo molto importante della disciplina

privacy GDPR ed è oggetto di vari accertamenti da parte dell’Autorità Garante, che ha riscontrato difformità rispetto a quanto previsto dall’art. 29 GDPR.

Il Titolare del trattamento deve osservare precise regole ordinarie anche per quanto concerne la nomina di responsabili ai sensi dell’art. 28 GDPR. Ed invero, qualora il Titolare del trattamento scelga di esternalizzare l’installazione del sistema di videosorveglianza ad una società terza, sarà necessario predisporre l’atto di nomina della stessa al fine di precisare le istruzioni per la gestione dei dati personali correlati alle attività di installazione, assistenza e manutenzione del sistema di videosorveglianza in funzione presso una società o un’azienda.

A titolo esemplificativo, tra gli adempimenti che dovranno essere indicati all’interno dell’atto di designazione possono annoverarsi nei confronti del soggetto nominato come Responsabile esterno quelli di: assicurare la predisposizione e l’aggiornamento di un sistema di sicurezza dei dati conforme alle misure adeguate prescritte dal Regolamento UE n. 679/2016 e dal Dlgs n.196/2003; assicurare e verificare che i dati personali oggetto del trattamento siano trattati in modo lecito e corretto, e comunque nel rispetto delle disposizioni GDPR e del novellato al Codice Privacy; garantire il rispetto dei tempi di conservazione delle videoregistrazioni previsti dalle specifiche autorizzazioni aziendali in materia di videosorveglianza.

5. La cd. videosorveglianza “domestica”: brevi cenni

Il 20 gennaio 2022 il Garante per la protezione dei dati personali ha pubblicato una scheda informativa volta a chiarire le regole e gli accorgimenti indispensabili da applicare ai sistemi di videosorveglianza domestica.

Poiché l’apposizione di telecamere a scopi domestici e personali può comportare un rischio di commissione del reato di interferenza illecita nella vita privata altrui *ex art. 615-bis c.p.*, assumono rilevanza fondamentale tali prescrizioni assunte dal Garante privacy in relazione al fatto che possono essere oggetto di ripresa soggetti che operano sia all’interno sia all’esterno di una privata abitazione.

Pertanto, le persone fisiche possono, anche nell’ambito di attività di carattere personale o domestico, attivare sistemi di videosorveglianza a tutela della sicurezza di persone o beni senza alcuna autorizzazione e formalità, purché:

- Le telecamere siano idonee a riprendere solo aree di propria esclusiva pertinenza.
- Vengano attivate misure tecniche per oscurare porzioni di immagini in tutti i casi in cui, per tutelare adeguatamente la sicurezza propria o dei propri beni, sia inevitabile riprendere parzialmente anche aree di terzi;
- Nei casi in cui sulle aree riprese insista una servitù di passaggio in capo a terzi, sia acquisito formalmente (una tantum) il consenso del soggetto titolare di tale diritto;
- Non siano oggetto di ripresa aree condominiali comuni o di terzi;
- Non siano oggetto di ripresa aree aperte al pubblico (strade pubbliche o aree di pubblico passaggio);
- Non siano oggetto di comunicazione a terzi o di diffusione le immagini riprese.

Come si evince dalla lettura di tali indicazioni, nonostante la possibilità di installare un sistema di videosorveglianza anche all'interno della propria proprietà privata, è chiaro il rinvio al principio di minimizzazione ex art. 5 del Regolamento GDPR, ai sensi del quale i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità di trattamento.

Il Garante ha previsto anche che debbano essere attivate misure tecniche atte a oscurare porzioni di immagini nei casi in cui, al fine di tutelare in modo adeguato la propria sicurezza e quella dei propri beni, sia inevitabile riprendere parzialmente aree di terzi, e che, in ogni caso le riprese non devono essere oggetto di comunicazione a terzi o di diffusione.

SEZIONE III
DIGITALIZZAZIONE, PRIVACY E PROCESSO

L'EVOLUZIONE DEL PROCESSO TRIBUTARIO

SOSPESO TRA CARTA E DIGITALE

Antonella D'Iorio

Abstract: L'importanza di un corretto trattamento dei dati significa anche una buona gestione delle informazioni e un adeguato governo degli archivi in un circolo virtuoso che riverserà, poi, i suoi frutti sugli atti e sulle attività da porre in essere.

Ciò è vero specialmente per l'ambito pubblico e, in particolar modo, determinante per le procedure di riscossione condotte dal Fisco nei confronti dei cittadini contribuenti. Se si considera che il contraddittorio che si va ad instaurare per le questioni tributarie tra soggetto pubblico e privato cittadino è puramente documentale sarà lampante che solo il rispetto delle norme e delle buone pratiche potrà determinare un modo corretto di agire. Avere metodo rafforzerà ogni altra capacità a saper impegnare bene le risorse disponibili con riferimento espresso anche all'impiego delle nuove tecnologie e all'informatizzazione documentale e delle procedure.

Diversamente saranno registrati impatti negativi e saranno messi in crisi quei principi fondamentali e quelle garanzie irrinunciabili di rilevanza costituzionale.

The importance of a correct data processing also means a good management of information and a governance of archives in a virtuous circle which will deliver advantages on the acts and activities to be implemented.

This is especially true for the public sphere and, in particular, it is crucial for the collection procedures conducted by tax authorities against tax-paying citizens.

If we consider that the debate, established for tax issues between public entities and private citizens, is purely documentary, it will be clear that only compliance with rules and good practices can determine a correct way of acting. Having a method will strengthen all the abilities to know how to employ the available resources with the specific reference to the use of new technologies and the computerization of documents and procedures.

If it were otherwise, negative impacts would be recorded and those fundamental principles and inalienable guarantees of constitutional relevance would be undermined.

Parole chiave: domicilio e notifica cartacea e digitale, procedure esecutive, scheda anagrafica del contribuente, PEC, relata di notifica, Statuto del contribuente, CAD, onere della prova.

Sommario: 1. Le disavventure di un contribuente: analisi del contesto - 2. Premessa generale sulle procedure esecutive - 3. La procedura coattiva in modalità cartacea. - 4. La procedura coattiva in modalità digitale - 5. La disciplina e l'onere della prova in materia di tributi - 6. Conclusioni

1. Le disavventure di un contribuente: analisi del contesto

Si affronta di seguito il caso di un cittadino che propone ricorso all'autorità giudiziaria per impugnare, in qualità di contribuente, un'iscrizione ipotecaria comunicatagli a mezzo posta elettronica certificata di importo superiore al valore di € 100.000,00 (centomila/00euro) quale pretesa creditoria che sarebbe stata originata dal succedersi nel tempo di una serie di atti impositivi non opposti nei termini di legge che avrebbero di fatto aggravato la posizione del contribuente. Quest'ultimo nega di averne avuto cognizione con notifica in modalità cartacea e deduce a sua difesa i seguenti motivi: a) l'inesistenza della notifica degli atti presupposti su cui si fonderebbe il pignoramento, b) la violazione dei fondamentali principi costituzionali della procedura azionata.

Pensare che la vicenda esaminata non rappresenta un caso unico ed eccezionale ma un esempio di una casistica più ampia di procedimenti esecutivi vessatori condotti con azioni irragionevoli, sproporzionate e non conformi ai principi di buon andamento ed imparzialità dell'azione amministrativa deve invitare a riflettere.

Con la presente trattazione, dunque, nell'esaminare una tra le principali procedure cautelari a tutela del credito attuata con il pignoramento verso terzi da parte dell'Agenzia delle Entrate, così come previsto dall'art. 72-bis D.P.R. 602/73 nei confronti del debitore cittadino contribuente, fa risaltare agli occhi l'evoluzione di una giustizia contesa tra una realtà analogica e digitale dai confini non ben delineati.

Sarebbe dunque opportuno che lo studioso contemporaneo si addentri nella materia con crescente sensibilità senza tralasciare dettagli e venature così che questi cambiamenti non vadano a rivelarsi segnali precursori di un collasso piuttosto che di un progresso.

2. Premessa generale sulle procedure esecutive

In via ordinaria, nelle procedure azionate per il recupero dei crediti, quando vi è assenza di volontà da parte del debitore ad adempiere ad una richiesta di pagamento dovuto, il creditore dovrà indispensabilmente munirsi di un provvedimento giurisdizionale che legittimi e caratterizzi la fase esecutiva da intraprendere per poter soddisfare la sua pretesa creditoria. Un classico esempio è l'avvio della procedura di recupero attraverso il decreto ingiuntivo ovvero la richiesta al giudice al fine di ottenere un titolo valido per l'esecuzione nei confronti del debitore.

Il rapporto con il Fisco, invece, trova la sua particolarità e giustificazione nella natura amministrativa dei titoli esecutivi tributari in quanto, a differenza della procedura esecutiva ordinaria, qui si esprime bene il potere della Pubblica Amministrazione di determinare effetti tipici di una espropriazione nei confronti del cittadino contri-

buente senza bisogno di dover passare attraverso l'autorità giudiziaria.

Perciò è il Fisco, al posto del giudice, ad ordinare direttamente al terzo (solitamente la banca o il datore di lavoro), di corrispondere a proprio favore le somme pignorate e non sarà necessario alcun provvedimento di assegnazione emesso dal giudice.

Questo sistema snello di riscossione coattiva fondato su un criterio di spiccata funzionalità a favore di un recupero delle somme vantate da un creditore speciale, quale è la Pubblica Amministrazione, che agisce a tutela del denaro pubblico viene però troppe volte a scontrarsi con altrettanti principi e ragioni che sono costituzionalmente garantiti e che non possono meritare di restare compressi e offesi da automatismi poco virtuosi come accade, primo tra tutti, nei confronti del diritto di difesa garantito all'art. 24 della nostra Carta costituzionale.

Pertanto, pur volendo riconoscere che dall'altra parte a procedere vi sia un soggetto privilegiato per le facilitazioni che possa meritare rispetto a un privato, non si può accettare, come nel caso che ci occupa, che venga elusa la legittimità della iscrizione nei ruoli esattoriali come nemmeno si può accettare la carenza di una prova valida ed incontestabile dell'esistenza giuridica e della regolare notificazione delle cartelle di pagamento¹.

Le norme che regolano la materia per l'ambito delle azioni esecutive e cautelari del credito hanno meritato nel tempo più interventi da parte del legislatore per riordinare una disciplina alquanto complessa e poco organica fino alla più recente riforma del processo tributario di cui alla Legge n. 130/2022 in vigore solo dallo scorso 16 settembre. Non va tralasciato, tuttavia, che in relazione alla formazione, gestione e conservazione dei documenti informatici il Codice dell'Amministrazione Digitale, introdotto con il d.lgs. n. 82/2005, aveva già risposto alle esigenze del processo tributario e, prima ancora, a quelle attività presupposte e basilari senza tuttavia riscuotere l'attenzione che meritava e restando di fatto ignorato da Avvocatura e Magistratura.

3. La procedura coattiva in modalità cartacea

L'onere probatorio su cui si incentra la procedura volta al recupero coattivo dei crediti incombe necessariamente sull'Agente della riscossione a partire dalla legittimità delle operazioni di notificazione che rappresentano l'avvio dell'iter esecutivo nella sua successione per fasi di crescente aggressività verso il contribuente.² Nel caso che ci occupa le cartelle esattoriali non sono state ritualmente notificate al debitore, né quando l'Agente di riscossione ha preferito la modalità di notificazione cartacea né quando si è avvalso delle comunicazioni informatiche a mezzo PEC, per-

¹ Come è vero nel rispetto degli articoli 137 - 148 c.p.c. in combinato disposto con l'art. 26 DPR 602/73 sulle cui basi poggia e si fonda il diritto di credito che si intende far valere

² È necessario che l'Agente della riscossione provi di aver ottemperato al dettato di legge ex artt. 138, 139, 140 c.p.c.

tanto il contribuente debitore non è stato messo perfettamente in grado di spiegare le proprie difese e nemmeno di eccepire tutte le circostanze che avrebbe potuto far valere a suo favore nei tempi utili consentiti. Tutto ciò costituisce, inevitabilmente, una grave violazione del diritto di difesa.

Non sarà pertanto sufficiente l'iscrizione a ruolo (in quanto atto meramente interno) a interrompere i termini per la riscossione ma è necessario un atto, avente carattere recettizio che metta effettivamente in mora il debitore.³

È adempimento dovuto dall'Agente della riscossione, per la notifica nella modalità cartacea al contribuente, la consegna della copia della cartella mentre il creditore (o il Concessionario che agisce per il creditore) conserverà ed esibirà l'originale, in quanto ne deve essere in possesso, al fine di ottenere la prova della conoscenza legale del contenuto degli atti.⁴

Nel caso di specie le operazioni di notifica non sono state indirizzate al domicilio fiscale che il contribuente aveva dichiarato sin dall'anno 2001, ma l'Ente ha preferito inviare l'atto ad un indirizzo diverso dal quale il contribuente, per necessari lavori di manutenzione straordinaria, si era già trasferito e costituente circostanza ben nota all'Agenzia delle Entrate in quanto depositaria della Scheda Anagrafica del contribuente.

A tal proposito va anche riferito che alla data delle suddette operazioni, alla vecchia residenza, non vi era alcun elemento riconducibile al contribuente.

La storica assenza assoluta di citofoni, campanelli e cassette postali, nega la possibilità di individuazione di chicchessia trattandosi di un fabbricato indipendente ed isolato. La notifica dell'atto in questione è del tutto inesistente, poiché è stata effettuata alla vecchia residenza del contribuente, fabbricato rimasto poi disabitato ed ove tra l'altro, non vi era alcuna altra persona capace e idonea a ritirare la posta.

Dagli atti consegnati integralmente soltanto all'accesso fisico del cittadino negli uffici, si è appurato che il messo dell'Agenzia delle Entrate si era recato sui luoghi inequivocabilmente disabitati e non trovandovi alcuno depositava nello stesso giorno il piego presso la casa comunale e, del tentativo di notifica del piego e del suo deposito, il messo ha inteso dare notizia al contribuente a cura dell'agente postale preposto alla consegna mediante avviso di comunicazione di avvenuto deposito in busta chiusa, a mezzo lettera raccomandata a/r con avviso di ricevimento e ciò sempre all'indirizzo ove non vi erano persone per il ritiro e tantomeno cassette postali ove custodire qualsivoglia plico o altro.

Il messo notificatore avrebbe svolto correttamente il suo dovere con la semplice verifica della scheda del contribuente in possesso dell'Agenzia delle Entrate dalla quale si rileva la residenza, il domicilio del ricorrente, e dalla semplice lettura avrebbe rilevato molto agevolmente la sede di lavoro del contribuente, peraltro, molto noto all'ufficio considerato che il contribuente in questione svolge la professione di avvocato.

Orbene, la notificazione in modalità cartacea, osserva la Suprema Corte di Cassazio-

³ La Corte di Cassazione lo ha stabilito con l'ordinanza n. 11605/21 del 4 maggio

⁴ Corte di Cassazione, Sez. Tributaria sentenza 11 febbraio 2015 n. 2625

ne, si ha per eseguita decorsi dieci giorni dalla data del rilascio, vale a dire dalla data dell'immissione, attestata dall'agente postale, nella cassetta della corrispondenza del destinatario dell'avviso di giacenza.⁵

Ma la notifica da parte dell'Agenzia delle Entrate è affetta da vizio di nullità insanabile e assolutamente inesistente poiché per il notificante il perfezionamento della notifica si ha per eseguita decorsi dieci giorni dalla data di spedizione tramite raccomandata dell'avviso di giacenza all'esatto indirizzo del destinatario⁶ ma l'indirizzo in questione non era esatto considerato pure che l'Ufficio precedente poteva facilmente ricavare tale verità usando la normale diligenza.

Dunque, non vi è nessuna prova fornita in ordine all'esistenza degli atti presupposti e prodromici da cui trae origine il ruolo esattoriale azionato che ha comportato l'iscrizione ipotecaria in danno del contribuente.

4. La procedura coattiva in modalità digitale.

Pur scontando la nullità ed inesistenza degli atti originari ed originali di cui vi è carenza assoluta di prova per l'attivazione di qualsivoglia pignoramento, gli importi richiesti venivano aggravati di spese, interessi, sanzioni permettendo un'iscrizione ipotecaria che veniva confezionata convertendosi dalla carta al digitale e passando dalla Agenzia delle Entrate all'Agenzia delle Entrate Riscossione (quest'ultima in veste di soggetto Concessionario).

Così, avvalendosi della trasmissione PEC, l'Agenzia delle Entrate Riscossione indirizzava alla casella del professionista le pretese creditorie aggiornate negli importi agendo a danno dell'immagine oltre che del patrimonio del contribuente.

Andrebbe certamente denunciata la violazione degli artt. 3 e 6 della L. 241/90 concernenti il dovere di motivazione del provvedimento e il rispetto degli obblighi che fanno capo al responsabile del procedimento che pare si sia fatto sfuggire parecchi dettagli sulla procedura in corso.

Per non dire poi che l'atto allegato a mezzo posta elettronica certificata era un file PDF mancante di firma digitale e il tutto era proveniente da un indirizzo PEC diverso da quello ufficiale indicato nel registro IPA. La PEC ricevuta è pervenuta, infatti, dall'indirizzo noreply.nomedellaregione.ipol@pec.agenziariscossione.gov.it, non avendo l'Amministrazione utilizzato la PEC attribuita all'Agenzia delle Entrate-Riscossione, presente nell'elenco ufficiale "IPA" (Indice delle Pubbliche Amministrazioni), ossia protocollo@pec.agenziariscossione.gov.it.

Proprio una recente Giurisprudenza⁷ ha sancito la nullità delle notifiche azionate a mezzo PEC dalla Agenzia delle Entrate Riscossioni aver "utilizzato un indirizzo PEC

⁵ Cass. Civ. 2047/2016.

⁶ Cass, civile 5347/2018 e n. 19958/2017.

⁷ CTP di Roma, sentenza n. 601/2020

sbagliato” ovvero non quello ufficiale e inserito nell’indice delle Pubbliche Amministrazioni quale “protocollo@pec.agenziaiscossione.gov.it” ma altro indirizzo, facendo sì che la notifica risultasse improduttiva di effetti giuridici e cioè come mai avvenuta.

È chiaro che tali prescrizioni non possono essere superate con il semplice riferire che l’atto ha raggiunto il suo scopo. Anzi, si pensi alla costante minaccia informatica che prende di mira maggiormente i siti web pubblici ed istituzionali e quanto il contribuente abbia la necessità e la diligenza di non avere in considerazione comunicazioni facilmente equivocabili o sospette. In definitiva, la prova, in astratto, della notifica delle cartelle può essere validamente offerta, anche per la modalità digitale, solamente con la produzione in giudizio dei documenti originari ed originali e/o soddisfacendo l’iter descritto delle norme che ne specificano anche gli obblighi e le modalità di conservazione con i log delle operazioni svolte.

5. La disciplina e l’onere della prova in materia di tributi

In conformità a quanto assunto innanzi si fa qui risaltare che il servizio di riscossione è tenuto per legge a conservare gli atti e a garantire l’accesso ai privati

Ai rappresentanti degli Enti è richiesto di “conformarsi ai principi dello Statuto dei diritti del contribuente di cui alla legge 27 luglio 2000 n. 212, con particolare riferimento ai principi di trasparenza, leale collaborazione e tutela dell’affidamento della buona fede, nonché agli obiettivi individuati dall’art. 6 della legge 11 marzo del 2014 n. 23, in materia di cooperazione rafforzata, riduzione degli adempimenti, assistenza e tutoraggio del contribuente”.⁸

La Giurisprudenza è intervenuta negli ultimi anni a chiarire che grava sulle amministrazioni, e non certo sul contribuente, l’onere di conservazione e produzione anche a mezzo stampa del duplicato della cartella generato dallo stesso ruolo riportante attestazione della conformità all’originale; anzi, grava sullo stesso Ente di riscossione organizzare i suoi uffici e le risorse interne per consentire ciò nel pieno rispetto dei principi di trasparenza ed efficienza.

Pertanto, la procedura di espropriazione esattoriale ed ogni cartella/intimazione a presupposto del pignoramento immobiliare ed iscrizione ipotecaria, di cui al caso riferito ed esaminato, risultano improcedibili ed illegittimi in quanto non azionabili senza dimostrazione della regolarità dei ruoli/cartelle/intimazioni presupposti così come sopra invocati.

Nel dettaglio, più precisamente va contestato alla Agenzia delle Entrate Riscossioni

⁸ Ai sensi del quinto comma dell’art. 1 del D.L. n. 193/2016

la disapplicazione delle norme e regole tecniche introdotte in materia di conservazione digitale con il DMEF 2014 (in G.U. del 26.06.2014) sulla disciplina dei documenti informatici fiscalmente rilevanti nonché in spregio di quanto già stabilito dal CAD all'art. 3 (Diritto all'uso delle tecnologie) e art. 3 - bis (Identità digitale e domicilio digitale) e ss. che in materia di notificazione al domicilio digitale stabiliscono le procedure per la corretta formazione degli atti nativi digitali da considerarsi quali documenti originali informatici a cui va apposta sottoscrizione con firma digitale o firma elettronica o firma qualificata avanzata con espresso obbligo di conservazione e tenuta nei propri archivi e laddove gli stessi documenti siano da inviare ai contribuenti nella forma, fino ad oggi intesa più tradizionale, che preveda la modalità cartacea a mezzo posta ordinaria o raccomandata con avviso di ricevimento, verrà utilizzata, indispensabilmente, la copia analogica dei suddetti documenti informatici sottoscritti con firma autografa sostituita a mezzo stampa e predisposta secondo le disposizioni di cui all'art. 3 del d.lgs. n. 39/1993.

Non esistono documenti nel mondo del diritto validi per legge se privi di firma e laddove vi è dispensa alla apposizione della firma - in virtù delle norme richiamate - va fatta espressa menzione in calce all'atto motivandone l'assenza stessa ai fini di legge. Allo stesso modo, non esistono nel mondo del diritto documenti che non debbano essere classificati ed archiviati. È perciò incoerente ogni altra teoria imbastita dalla Agenzia delle Entrate Riscossione per aggirare il corretto iter nel porre in essere il suo operato.

Ed invero ed in virtù del principio di trasparenza e pubblicità degli atti non si possono addurre simili scusanti a discarico per la posizione rivestita di Ente pubblico economico e, dunque, in riferimento a un ruolo che conferisce la qualità di parte integrante dell'amministrazione finanziaria dello Stato, come previsto con D.L. n. 193/2016, e che è pertanto Ente strumentale dell'Agenzia delle Entrate, sottoposto all'indirizzo ed alla vigilanza del Ministro dell'Economia e delle Finanze nonché al controllo della Corte dei Conti sulla gestione finanziaria ai sensi degli art. 2 e 3 della Legge n. 259/1958.

Si osserva altresì sull'onere probatorio assolto con le relate che le stesse non possono essere rappresentate da copie ritagliate di relate disgiunte dalle corrispondenti cartelle, prive della indicazione finanche del nome del mittente e destinatario dell'atto, oltre che dell'attestazione del numero delle pagine del presunto atto notificato e di cui non è dato conoscere il contenuto.

Tali documenti, infatti, non sarebbero conformi al modello legale di relata di notifica, ponendosi in contrasto anche con gli artt. 125 e 137, 148 e 156 c.p.c. e con l'art. 60 dello Statuto del Contribuente di cui al D.P.R. n. 600/1973. Nel caso di incompleta esibizione, a nulla rileva il numero stampato sulle presunte relate, solo in astratto riconducibili ad un plico, forse contenente un atto o documento che non si capisce a chi è destinato o consegnato, di cui, inoltre, non è dato conoscere neanche il numero

delle pagine, il colore, il contenuto e la motivazione⁹.

La relata disgiunta non dimostra, dunque, quale sia l'atto notificato e chi sia il destinatario del provvedimento, con la conseguenza, tra l'altro, che non assume alcuna rilevanza l'indicazione della sola qualifica del consegnatario, potendo questi essere il parente o l'addetto alla ricezione di un qualsivoglia contribuente italiano. Inoltre, la prova della relata di notifica delle cartelle o di altre intimazioni non può essere rappresentata da una semplice fotocopia, ovvero da un documento non munito di alcuna attestazione di autenticità proveniente da un pubblico ufficiale. Peraltro, le "copie" di relate di notifiche solitamente prodotte in atti dall'Agente della riscossione, scaturiscono da un procedimento interno di "scannerizzazione", non governato da un pubblico ufficiale, procedimento, quindi che non garantisce una prova certa della corrispondenza tra il documento informatico (poi riprodotto in forma cartacea per le esigenze processuali) e l'originale.¹⁰

Per questi motivi, l'eventuale documentazione prodotta in copia merita di essere espressamente disconosciuta dal contribuente, ai sensi degli artt. 215 c.p.c. e 2719 c.c., in quanto neanche fotocopie degli atti opposti ma cartule difformi.

Del resto tale conclusione si ricollega direttamente a ciò che è effettivamente un estratto di ruolo: una mera riproduzione, solo parziale, del più ampio contenuto della propedeutica cartella.

A tale conclusione perviene anche la consolidata giurisprudenza di legittimità e di merito¹¹ affermando il seguente principio: *le copie fotografiche o fotostatiche di un documento hanno, a norma dell'art. 2719 c.c., lo stesso valore probatorio degli originali quando la loro conformità è attestata dal pubblico ufficiale, ovvero non è espressamente disconosciuta dalla parte contro cui sono prodotte, con la conseguenza che, in caso di disconoscimento della copia non autenticata, questa non può essere utilizzata come prova dei fatti in essa rappresentati né dell'esistenza stessa della scrittura riprodotta.*

Anche in virtù del principio dell'onere della prova, contemplato dall'articolo 2697 c.c., l'onere della prova spetta a chi vuole fare valere un diritto e non a chi lo nega. Per cui, il creditore, ha l'obbligo di dimostrare la validità del credito vantato, esibendo in giudizio gli originali delle presunte cartelle/avvisi con in calce le rispettive relate, attestanti l'esistenza e la regolare notifica degli stessi come per legge.

Alla luce di quanto detto, dunque, è importante evidenziare ancora una volta che l'Agenzia delle Entrate Riscossione è chiamata ad assolvere ad un doppio onere probatorio, ossia:

1. provare la NOTIFICA delle cartelle/avvisi, attraverso la produzione in giudizio delle relate in calce all'atto originario ed originale assunto per notificato;
2. provare il CONTENUTO delle cartelle, attraverso la produzione in giudizio di copia degli atti originari notificati al contribuente.

⁹ Cass. n. 2526 11 febbraio 2015

¹⁰ Cass. sent. n. 23213/14

¹¹ CASS. SEZ. UNITE 12244/09 e Corte d'Appello di Napoli Sez. II 03/02/2009

Solo grazie a questa documentazione si potrà dimostrare la piena legittimità delle cartelle di pagamento e quindi delle pretese avanzate nei confronti del contribuente.

6. Conclusioni

È pratica diffusa nella riscossione degli ultimi anni quella di azionare contemporaneamente più procedimenti anche per il recupero di un unico e modesto debito determinando un vero e proprio abuso di diritto e abuso di quegli strumenti che l'ordinamento mette a disposizione del Fisco nei limiti di una corretta tutela del suo interesse sostanziale.

E considerato che, anche sotto un aspetto esclusivamente organizzativo, non si è ancora completata la transizione verso una cultura completamente digitale, il rischio è che nel guado si indeboliscano anche i principi indiscutibili del nostro ordinamento giuridico ottenendo come risultato una somma distruttiva piuttosto che virtuosa delle caratteristiche dei due mondi.

In riferimento all'atto dell'iscrizione di ipoteca che è oggetto di questa trattazione, il contribuente è riuscito provvidenzialmente a fornire tutta la documentazione necessaria affinché si procedesse allo sgravio di quasi tutte le cartelle ed avvisi di accertamento da cui era scaturita l'ipoteca per un importo di gran lunga superiore rispetto ad una pretesa creditoria che potesse dirsi eventualmente dovuta.

Non potevano perciò valere le giustificazioni e scusanti addotte dalla Agenzia di Riscossione con una procedura messa in essere, come nel caso di specie, su basi infondate, criptiche e generiche con pretese di pagamento carenti di qualsivoglia prova e senza alcuna indicazione delle corrispettive cartelle mai ritualmente notificate oltre che prive di motivazione, prova e sottoscrizione come per legge e ciò anche in conformità al recentissimo orientamento affermato dalla Suprema Corte¹².

Con la riforma del processo tributario in vigore dallo scorso settembre e introdotta definitivamente da gennaio 2023 oggi la novità più rilevante è rappresentata dall'introduzione di magistrati tributari scelti per concorso e con obbligo di formazione permanente. L'auspicio è che questo possa favorire un approccio alla materia garantiti da competenze di qualità superiore e con la fiducia che indirettamente ciò possa tornare utile anche per incentivare nel modo migliore gli uffici preposti all'esecuzione al di fuori delle aule processuali.

¹² Corte di Cass. SS. UU. n. 10012 depositata il 15 aprile 2021

LA RIFORMA CARTABIA E LA SPECIFICA APPLICAZIONE DEL DIRITTO ALL'OBLIO AGLI IMPUTATI O AI SOGGETTI ASSOGGETTATI AD INDAGINI

Simonetta Zingarelli

Abstract: La legge 27 settembre 2021 n. 134 rubricata “Delega al Governo per l’efficienza del processo penale nonché’ in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari”, conosciuta come “riforma Cartabia”, prevede all’art. 1, comma 25, la delega al Governo ad adottare i decreti legislativi di modifica al codice e procedura penale e alle norme di attuazione che consenta in caso di “...*decreto di archiviazione il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l’emissione di un provvedimento di deindicizzazione che, nel rispetto della normativa dell’Unione europea in materia di dati personali, garantisca in modo effettivo il diritto all’oblio degli indagati o imputati*”. Sulla base di tale norma è stato introdotto l’art. 64 ter, nel D.Lgs. 271/1989 (Norme di attuazione del Codice Penale).

The law of 27 September 2021 n. 134 entitled “Delegation to the Government for the efficiency of the criminal process as well as in the field of restorative justice and provisions for the rapid definition of judicial proceedings”, known as the “Cartabia reform”, provides in art. 1, paragraph 25, the delegation to the Government to adopt the legislative decrees amending the penal code and procedure and the implementing rules that “the filing decree and the order not to proceed or acquittal sentence constitute grounds for a de – indexation measure which, in compliance with European Union legislation on personal data, effectively guarantees the right to be forgotten of suspects or accused persons”. On the basis of this provision, the art. 64 ter, in Legislative Decree 271/1989 (Implementing rules of the Criminal Procedure Code).

Parole chiave: Diritto all’oblio *degli imputati e delle persone sottoposte ad indagini*, deindicizzazione, Riforma Cartabia.

Sommario: 1 Introduzione - 2 Breve excursus giuridico del diritto all’oblio - 3 L’art. 64 ter - *Diritto all’oblio degli imputati e delle persone sottoposte ad indagini* – delle disposizioni di attuazione del codice di procedura penale – Conclusioni.

1. Introduzione

L'introduzione dell'articolo 64 ter¹ nelle norme di attuazione del Codice Penale, ha previsto un' importante, ulteriore specificazione del diritto all'oblio rispetto a quanto già stabilito dall'art. 17 del Reg. UE 679/2016. Per quei soggetti imputati o persone sottoposte ad indagine nell'ambito del procedimento penale verso le quali viene disposto un provvedimento di proscioglimento o di non luogo a procedere, la norma prevede la possibilità di **deindicizzare, sulla rete internet, i dati personale trattati**. Naturalmente è necessario fare riferimento ad alcuni principi relativi al diritto di "rimanere anonimi" già introdotti dalle precedenti norme dal Reg. UE 2016/679 (Regolamento generale sulla protezione dei dati). È chiaro, inoltre, che l'applicazione del diritto all'oblio ha dovuto sempre nel tempo cercare di ponderare e di trovare un equilibrio tra tutte le parti, **doendosi contemperare, appunto, i diversi interessi**: quello del titolare a rendere "pubbliche" determinate informazioni e quello degli interessati a tutelare i propri dati anche attraverso la deindicizzazione dai motori di ricerca, in virtù del trascorre del tempo.

2. Breve excursus giuridico del diritto all'oblio

Per comprendere appieno la portata della norma in esame è giusto fare un cenno a cosa si intende per **diritto all'oblio** e **deindicizzazione** dei dati personali trattati. Il problema del diritto alla riservatezza si pone fin dalla fine dell'Ottocento con l'articolo "The right to privacy" (il diritto ad essere lasciato solo) di Warren e Brandeis. Ai primi del '900 in Europa prima e poi in Italia poi verso gli anni 50, il diritto alla riservatezza viene introdotto soprattutto con riferimento, ad esempio, a pellicole cinematografiche in cui si raccontava la vita privata di artisti e dei quali si poteva ledere la privacy dei protagonisti delle storie. Certamente, però, i dati anche sensibili degli interessati avevano una diffusione più ristretta rispetto al successivo avvento del World wide web. È, infatti, dagli anni '70 con l'utilizzo dei computer, sia nell'ambito pubblico, che privato, che comincia a diventare importante il peso di **un possibile controllo dei dati personali cosiddetti "sensibili"** riguardanti, per esempio, le origini razziali o le opinioni politiche.²

La necessità di una maggior tutela dei dati personali e quindi l'esigenza di trovare un equilibrio tra diritti fondamentali come la libertà di informazione ed espressione, da una parte, e la tutela dei dati personali dall'altra, ha richiesto una specifica normativa. Negli anni '90 con l'avvento di Internet, utilizzato da buona parte della popolazione, anche il Legislatore italiano comincia a preoccuparsi di normare spe-

¹ L'art. 64 ter, è stato introdotto dall'art. 41, comma 3, lett. H) del D.Lgs. 150/2022, in applicazione di quanto previsto dalla L. 134/2021.

² Giovanni Pascuzzi, Il diritto dell'era digitale, casa editrice Il Mulino 2006.

cificatamente gli aspetti legati alla privacy³ con la L. 675/96 che confluirà poi nel D.Lgs. 196/03.⁴

Il problema su cui occorre porre l'attenzione è quello di **prevenire il pericolo della diffusione** delle notizie e informazioni contenenti i dati personali derivante dalla rivoluzione digitale e, quindi, riguarda non più il diritto ad essere lasciati soli, ma quello di **riuscire a controllare i propri dati personali**. La questione della tutela del trattamento dei dati personali in relazione al diritto all'oblio si pone certamente con riferimento alla **diffusione in rete dei dati**, rispetto anche ai procedimenti di tipo giudiziario e a fatti di cronaca che assumono un risalto maggiore rispetto al periodo in cui, la pubblicazione di notizie o informazioni avveniva sui quotidiani o riviste cartacee magari anche specializzate. È in quest'ambito che il diritto all'oblio deve essere inteso come la necessità non di non vedere pubblicate le vicende e le notizie relative ai propri dati legittimamente diffusi, ma piuttosto **la legittimità della permanenza sul web e/o la ripubblicazione delle stesse attraverso i motori di ricerca anche dopo il trascorrere di diverso tempo e il cambiamento delle situazioni** rispetto ai fatti riportati e pubblicati.⁵

È, con l'entrata in vigore del **Reg. UE 679/2016** che si fa esplicito riferimento, anche dopo copiosa giurisprudenza europea⁶, al diritto all'oblio.

La norma di cui all'art. 17 del Reg. UE 679/2016 ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice Privacy. L'articolo rubricato "*diritto alla cancellazione (diritto all'oblio)*", stabilisce che **l'interessato ha diritto di rettificare i dati o anche di vedere cancellati i propri dati nel caso in cui non siano necessari per le finalità per cui sono stati raccolti**, qualora l'interessato abbia revocato il consenso o sia opposto al trattamento dei dati personali che lo riguardano o il trattamento non sia a norma con il Regolamento. L'articolo in esame prevede, inoltre, con l'intento di rafforzare il diritto all'oblio, che il titolare del trattamento dei dati personali informi gli altri titolari a cancellare qualsiasi link, copia o riproduzione di tali dati personali.

Naturalmente, la norma prevede anche i casi in cui, invece, si ritiene possibile che il titolare continui a conservare i dati quando gli stessi siano trattati per un obbligo legale per un interesse pubblico o per il diritto ad esercitare la libertà di informazione. La possibilità di esercitare il diritto all'oblio consente, dunque, all'interessato, qualora ciò sia previsto dalla normativa di poter controllare i propri dati e far sì che noti-

³ Legge del 31 dicembre 1996 n. 675 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali - susseguente alla direttiva 95/46/ CE.

⁴ Si veda in tal senso l'art. 7 del D.Lgs. 196/06 in cui l'interessato poteva ottenere l'aggiornamento, rettificazione e l'integrazione, ma anche la cancellazione o la trasformazione in forma anonima per i dati trattati in violazione di legge.

⁵ Giusella Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità ne Il diritto all'oblio su internet dopo la sentenza google spain*

⁶ La più importante tra tutte Sentenza 13 maggio 2014 con la sentenza n. 317 - Corte di Giustizia (Sentenza Google Spain).

zie e informazioni risalenti nel tempo **non vengono più associate alla sua persona** quando ciò è previsto dalla norma nella specifica esplicitazione del diritto all'oblio.

3 L'art. 64 ter - *Diritto all'oblio degli imputati e delle persone sottoposte ad indagini* – delle disposizioni di attuazione del codice di procedura penale

Per entrare più nel dettaglio, in merito alla introduzione dell'art. 64 ter, l'articolo prevede il diritto degli imputati e delle persone sottoposte ad indagini **verso i quali è stata pronunciata una sentenza di proscioglimento o di non luogo a procedere** ovvero un provvedimento di archiviazione, la possibilità di chiedere la preclusione dell'indicizzazione o la deindicizzazione sulla rete internet dei propri dati personali presenti sul provvedimento sulla base di quanto previsto dall'articolo 17 del Reg. UE 769/2016. I commi successivi prevedono nello specifico: *nel caso di richiesta volta a precludere l'indicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi del presente articolo: «Ai sensi e nei limiti dell'articolo 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016⁷, è preclusa l'indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante.»*. 3. *Nel caso di richiesta volta ad ottenere la deindicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi del presente articolo: «Il presente provvedimento costituisce titolo per ottenere, ai sensi e nei limiti dell'articolo 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, un provvedimento di sottrazione dell'indicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal nominativo dell'istante.*

Attraverso la **deindicizzazione**⁸ si attiva un rimedio idoneo ad evitare che il nome della persona sia associato alle informazioni rilevabili su internet attraverso il motore di ricerca. Sostanzialmente attraverso la deindicizzazione le ricerche relative al nome dell'interessato non vengono associate direttamente al nome dello stesso e dunque ad episodi della sua vita passata anche se restano pubblicate perché rico-

⁷ Reperibile al seguente link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679> [2023]

⁸ Il diritto all'oblio su internet dopo la sentenza Google Spain a cura di Giorgio Resta e Vincenzo Zeno-Zencovich- Roma Trepress.

nosciuto un interesse in tal senso. Dunque, lo scopo della deindicizzazione è quello di non consentire che la persona sia trovata facilmente in relazione a quel tipo di episodio l'interessato voglia evitare che sia direttamente collegato alla sua persona. È stato in proposito sottolineato, sempre dalla Corte di giustizia, che *“l’organizzazione e l’aggregazione delle informazioni pubblicate su internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l’accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l’elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su internet, che consente loro di stabilire un profilo più o meno dettagliato di quest’ultima”*⁹ (Corte giust. UE, Google Spain e Google, cit., 37). **La deindicizzazione non consente all’interessato di essere completamente dimenticato, ma piuttosto di evitare che quelle informazioni siano immediatamente collegate alla sua persona.** Quindi grazie a questo strumento il nome dell’interessato non sarà direttamente collegato ai provvedimenti di cui all’art. 64 ter. La deindicizzazione consente, il contemperamento dei vari interessi in gioco e cioè da un lato evitare che dei fatti del passato siano direttamente associati all’interessato e dall’altro lasciare la notizia sul web e non eliminarla completamente poiché vi è un interesse da parte dei titolari del trattamento a lasciare on line¹⁰. *Le richieste di deindicizzazione non comportano la cancellazione completa dei dati personali. Infatti, i dati personali non saranno cancellati né dal sito web di origine né dall’indice e dalla cache del fornitore del motore di ricerca. Ad esempio, un interessato può richiedere la rimozione dall’indice di un motore di ricerca di dati personali provenienti da un mezzo di comunicazione, quale un articolo di giornale. In questo caso, il link ai dati personali può essere rimosso dall’indice del motore di ricerca, ma l’articolo in questione resterà comunque sotto il controllo del mezzo di comunicazione e può rimanere pubblicamente disponibile e accessibile, sebbene non sia più visibile nei risultati di ricerca basati sulle interrogazioni che includono, in linea di principio, il nome dell’interessato*¹¹.

L’articolo, al secondo comma specifica che la richiesta da parte del soggetto interessato dovrà essere proposta alla cancelleria di riferimento e sarà, dunque, il cancelliere del giudice che ha emesso il provvedimento ad apporre la dicitura prevista dalla norma¹².

⁹ Corte giust. UE, Google Spain e Google, cit., 37

¹⁰ Si veda in tal senso <https://ntplusdiritto.ilsole24ore.com/art/il-diritto-oblio-imputato-riforma-cartabia-AExO3QkC> - Il diritto all’oblio dell’imputato nella Riforma Cartabia – Pietro Montella.

¹¹ Linee guida 5/2019 sui criteri per l’esercizio del diritto all’oblio nel caso dei motori di ricerca, ai sensi del RGPD.

¹² «Ai sensi e nei limiti dell’articolo 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, è preclusa l’indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell’istante».

4 Conclusioni

La norma in esame assume importanza per diversi motivi, innanzitutto per quanto detto su innanzi relativamente alla possibilità di non associare in maniera diretta un evento diffuso su internet al proprio nome, che in ambito di provvedimenti giudiziari assume senza dubbio un'importanza maggiore con riferimento al desiderio di riservatezza su certi eventi della propria vita passata, ma assume rilevanza anche da un punto di vista procedurale, perché consente al soggetto interessato di rivolgere le proprie pretese direttamente alla cancelleria, presumibilmente per cercare di accelerare i tempi per ottenere la preclusione della indicizzazione o deindicizzazione rispetto ai provvedimenti previsti dal comma 1 dell'art. 64 ter. Per il resto però è anche da sottolineare che la norma non specifica cosa avvenga successivamente all'emissione del provvedimento, anche da parte del cancelliere, per esempio in caso di mancato rispetto dell'adempimento da parte dei motori di ricerca. Si dovrà, dunque, aspettare e capire l'orientamento della giurisprudenza e del legislatore in tal senso¹³.

¹³ Si veda in tal senso <https://www.agendadigitale.eu/documenti/giustizia-digitale/diritto-alloblio-d-ora-deindicizzazione-piu-facile-cosa-cambia-con-la-riforma-cartabia/> - Diritto all'oblio, da ora deindicizzazione più facile: cosa cambia con la riforma Cartabia – Fulvio Sarzana.

