


UNIVERSITÀ DEGLI STUDI DI MACERATA

DIPARTIMENTO DI STUDI UMANISTICI

CORSO DI DOTTORATO DI RICERCA IN
STUDI LINGUISTICI, FILOLOGICI, LETTERARI
CURRICULUM MEMORIE E DIGITAL HUMANITIES

CICLO XXXIV

Disposizioni normative, modelli e strumenti per la conservazione di documenti e archivi digitali in Italia e in Europa: panorama complessivo, casi di studio, analisi comparata e prospettive

RELATORE
Chiar.mo Prof. Stefano Pigliapoco

DOTTORANDO
Dott.ssa Federica Marti

COORDINATORE
Chiar.ma Prof.ssa Patrizia Oppici

ANNO 2022

Indice

Premessa

La riflessione sul tema della conservazione digitale, in particolare declinata sull'analisi comparativa in contesto europeo, costituisce, allo stesso tempo, un'importante azione di valutazione critica necessaria al superamento di problematiche e al miglioramento del proprio panorama di riferimento e un esercizio complesso di comprensione e vaglio di situazioni e contesti diversificati.

In questo particolare momento storico, lo sviluppo del tema non è certo agli albori, tuttavia alcuni aspetti si presentano ancora in via di definizione, altri in fase di consolidamento. Infatti, tanto in Italia quanto in Europa, il dibattito terminologico e concettuale è ancora in corso: l'ampio ambito cui il tema afferisce, che va dall'archivistica alle dinamiche amministrative, dall'intervento di gruppi di lavoro accademici a quelli riuniti al fine di produrre leggi e norme, nonché la diversità degli oggetti da conservare – espressione della varietà di soggetti con esigenze di conservare il proprio patrimonio digitale – rappresenta un'interdisciplinarità che rende complesso giungere a perimetri di compromesso.

Per quanto riguarda le metodologie e le applicazioni, invece, la parola chiave è *standardizzazione*: il fine condiviso di disporre a lungo termine dei *records* con le loro proprietà e le caratteristiche di integrità, autorità, stabilità, intellegibilità e accessibilità e l'esigenza, per raggiungere tale scopo, di implementare sistemi di conservazione architetturalmente lineari, interoperabili e non soggetti a obsolescenza tecnologica repentina, mostra, da un lato, un contesto sempre in evoluzione per via della rapidità con cui si susseguono le innovazioni ITC e l'attività della comunità di riferimento, dall'altro l'adozione di un insieme di standard e linee guida ormai condivise e solide, ma sottoposte ad aggiornamento costante.

Ciò premesso, il presente elaborato si propone, in primo luogo, di fornire un quadro sistematico e il più esaustivo possibile di ciò che ruota attorno alla conservazione digitale in Europa e in Italia, dal punto di vista della ricerca e a livello normativo: l'obiettivo è disporre di una panoramica su ciò che concerne le iniziative, le associazioni, i progetti, le soluzioni tecnologiche, gli strumenti, i modelli, le metodologie e la normativa (Parte I. *Digital preservation* in ambito europeo e Parte II. Conservazione digitale in Italia).

La Parte III dell'elaborato si concentra, invece, sulla descrizione dei casi di studio, selezionati sulla base di interessi specifici e contingenze di ricerca intervenute nel corso del progetto di dottorato. Va evidenziata preliminarmente, in relazione a questa particolare attività di rilevazione di contesti, una condizione valida anche per l'interpretazione dell'approccio con cui si è affrontata la prima parte del lavoro, ovvero la natura e a tematica vincolata del progetto di dottorato EUREKA[1] di cui questa tesi è espressione: la ricerca applicata svolta presso Namirial S.p.A.[2] ha determinato, innanzitutto, la forma della ricerca stessa, ma anche il prevalere dell'approfondimento di alcuni aspetti su altri, come l'analisi delle prassi di accreditamento all'estero per il riconoscimento dello status di *qualified long-term archiving services provider*[3].

Del campione rappresentato fanno parte l'Austria, la Francia, l'Olanda e la Romania; l'analisi di ogni caso di studio si compone di una parte introduttiva, della contestualizzazione delle problematiche inerenti alla conservazione digitale tra le autorità e gli enti amministrativi competenti, della descrizione della normativa vigente in materia e dell'esposizione di modelli e progetti sul tema.

La disamina di questi casi di studio, unita al quadro relativo agli ambiti europeo e italiano, è finalizzata ad effettuare l'analisi comparativa (che chiude tale lavoro di tesi): questa,

[1] I progetti di dottorato di tipo EUREKA, i cui temi sono il risultato dell'integrazione degli intenti di università, Regione Marche e aziende del territorio, hanno lo scopo di coniugare la ricerca accademica all'ambito imprenditoriale, con duplice finalità di fornire un risvolto applicato alle elaborazioni teoriche sviluppate in contesto universitario e di favorire l'innovazione delle aziende locali; questo programma nasce nell'ambito del POR Marche FSE 2014/2020, Asse 1- P.I. 8.1- R.A. 8.5 ed è attivo dal XXVIII ciclo di dottorato <https://www.unimc.it/it/dottorato-di-ricerca/phd-e-ricerca-applicata/programma-regione-marche-eureka>. Il presente progetto si riferisce al bando emesso dalla Regione Marche nel 2018, consultabile al link <https://bandi.regione.marche.it/Allegati/906/DDPF%20n%20673_2018.pdf>, recepito dall'Università di Macerata e dall'azienda Namirial S.p.A.

[2] Namirial S.p.A. nasce come società informatica di servizi nel 2000, fondata dagli imprenditori Claudio Gabellini ed Enrico Giacomelli allo scopo di investire nella trasformazione digitale del business. È, allo stesso tempo, un'azienda produttrice di soluzioni software e Certification Authority, che fornisce servizi fiduciari digitali come firme elettroniche, posta elettronica certificata, fatturazione elettronica e conservazione digitale a lungo termine. Namirial conta clienti e partner di molte aziende che operano nei settori di: servizi bancari, assicurazioni, energia, servizi pubblici, aziende farmaceutiche, manifattura, telecomunicazioni, distribuzione commerciale, ambiente, certificazioni, sicurezza, costruzioni, sanità, Pubblica Amministrazione, sindacati e associazioni professionali. La sede centrale si trova a Senigallia, con filiali operative e commerciali in Italia, Germania, Austria, Romania e Brasile, che servono clienti situati in Europa, Nord America, Sud America, Medio Oriente, Asia e Africa <https://www.namirial.com/it/>.

[3] A tal proposito, si cita testualmente la tematica vincolata del progetto, ovvero "Rilevamento in Italia e nei Paesi europei di modelli, strumenti e disposizioni normative per la conservazione di documenti informatici ed archivi digitali di enti pubblici ed imprese, effettuato con l'obiettivo di produrre un'analisi comparata e formulare proposte di miglioramento della realtà italiana".

introdotta da considerazioni generali sul contesto italiano, è volta a evidenziare criticità e punti di forza, in modo tale da far emergere potenzialità di miglioramento (Parte IV. Analisi comparativa).

Si correda l'elaborato con tre appendici, in cui si collocano i siti consultati per la ricostruzione dei contesti istituzionali e i quadri normativo e degli standard (Appendice A. Siti istituzionali consultati, Appendice B. Fonti normative citate, Appendice C. Norme e standard citati).

Parte I. La *Digital preservation* in ambito europeo

I.1 I documenti e gli archivi digitali tra ricerca e normativa

La riflessione sulla sopravvivenza nel tempo degli archivi e dei documenti digitali in ambito europeo[1] ha origine dalla percezione delle loro caratteristiche come più 'labili' rispetto a quelli analogici e, allo stesso tempo, dalla necessità del loro mantenimento a lungo termine:

> la sfida è molto impegnativa, non solo e forse non tanto sul piano tecnologico, bensì sul piano concettuale, perché i nuovi cambiamenti richiedono il radicale ripensamento della funzione di conservazione ma anche un aggiornamento costante che tenga conto della dinamicità dei nuovi scenari, come ci ricordano i progetti di ricerca che da più di un decennio si dedicano al problema. A differenza della dimensione statica e terminale che caratterizzava l'ambiente tradizionale, la conservazione digitale si confronta con il cambiamento costante della tecnologia e ha necessità di condividere con il mondo accademico impegnative attività di ricerca, di maturare esperienze e di tradurre entrambe in raccomandazioni operative e pratiche consolidate e spendibili[2].

A tal proposito, la progressiva digitalizzazione dei documenti e dei processi per produrli, gestirli e conservarli ha innescato, a partire dalla fine degli anni novanta, l'avvio della discussione sul tema, con focus in particolare sulle questioni inerenti al mantenimento dell'autorità dei *records*, che interessa sia l'ambito della ricerca sia l'ambito normativo.

In primo luogo, il quadro internazionale dei progetti, delle iniziative e dei gruppi di lavoro, da allora, ha fornito non solo elementi di riflessione teorica e concettuale, ma anche linee guida operative e strumenti applicativi effettivi[3]. La *digital preservation*, viene definita come «the specific process of maintaining digital materials during and across different

[1] Per ambito europeo, in questa sede, si vuole intendere il 'complesso' territoriale dell'Unione Europea (Regno Unito compreso: il presente elaborato si colloca temporalmente in un momento contemporaneo alle dinamiche Brexit), con riferimento all'insieme generale.

[2] M. Guercio, *Conservare il digitale. Principi, metodi e procedure per la conservazione a lungo termine di documenti digitali*, Roma, Editori Laterza; 2013, p. 9.

[3] M. Guercio, *Conservare il digitale: modello nazionale e contesto internazionale*, «DigitCult – Scientific Journal on Digital Cultures», 1 (2016), 2, pp. 20-21, disponibile online al sito <https://digitcult.lim.di.unimi.it/index.php/dc/article/view/10/10>. Si vedano i riferimenti concreti nel capitolo I.3.

generations of technology over time, irrespective where they reside[4]» e integrata col concetto di *records preservation*, ovvero «*the whole of the principles, policies, rules and strategies that controls the physical and technological stabilization and protection of the intellectual form of acquired records intended for their continuing, enduring, stable, lasting, uninterrupted and unbroken chain of preservation, without a foreseeable end*[5]»; in particolare, vengono sviluppati gli aspetti di strategia, intesa come set coerente di obiettivi e metodi per proteggere e mantenere le componenti digitali e le relative informazioni dei *records* acquisiti nel tempo e per riprodurre gli stessi autentici oggetti o aggregazioni archivistiche[6], e di sistema, ovvero l'insieme di regole che governano la conservazione intellettuale e perenne dei *records* acquisiti e gli strumenti e meccanismi utilizzati per implementare tali regole[7].

Inoltre, riguardo al mantenimento delle caratteristiche e dello stabilire delle regole, si mette in evidenza il già accennato duplice aspetto che caratterizza il documento archivistico, sia esso in formato analogico o elettronico: da un lato, la sua gestione è soggetta a vincoli di tipo amministrativo-legali, che lo sottopongono alla normativa di settore, civile, fiscale, e così via e che lo proiettano verso le discussioni di tipo giuridico; dall'altro, il passaggio alla fase storica lo introduce nell'ambito del beni culturali *tout-court*, rendendolo oggetto dei già citati progetti di ricerca e iniziative volte a preservarne il valore di memoria per i posteri e a promuoverne la diffusione.

Questo sfocia in un 'dualismo' tra dimensione giuridica e culturale che, a livello generale europeo, consiste nel fatto che iniziative e normativa non procedono di pari passo nella definizione e risoluzione delle problematiche e delle criticità. Ciò è dovuto a molteplici fattori, il cui filo conduttore è rappresentato dallo 'scollamento' tra gli aspetti sopra richiamati: nell'ambito della ricerca è prevalente – ma non esclusiva – l'elaborazione di strumenti e riflessioni *ex post*, che includono la conservazione dei documenti digitali nel più ampio ambito del patrimonio culturale digitale, mentre la normativa comunitaria,

[4] L. Duranti, R. Preston, *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Padova, Associazione Nazionale Archivistica Italiana, 2008, p. 784 disponibile online al sito <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf>.

[5] Ivi, p. 808.

[6] *Ibidem*.

[7] *Ibidem*.

concentrandosi su esigenze di tutela del consumatore e dell'utente e di mercato, non include, attualmente, un provvedimento specifico per la conservazione digitale. Le implicazioni sono evidenti nel fatto che ciascuno Stato europeo, avendo autonomia nell'emanazione di provvedimenti, ha la facoltà di istituire le proprie modalità organizzative, i propri schemi di requisiti e il proprio modello per l'implementazione dei sistemi di conservazione digitale[8].

Dunque, in questa prima parte sul contesto generale europeo, si vuole dare contezza da un lato del contesto normativo comunitario entro i cui confini si determinano le soluzioni adottate da ciascuno Stato per prassi e provvedimenti sulla tenuta degli archivi digitali, dall'altro dello stato dell'arte sulla conservazione digitale dal punto di vista della ricerca collegata a iniziative, associazioni, gruppi di lavoro e progetti.

[8] Questo tema verrà sviluppato nella Parte III, attraverso la descrizione dei casi di studio, e nella parte IV, con le riflessioni comparative su questi contesti.

I.2 Il perimetro normativo comunitario: provvedimenti delimitanti l'ambito della conservazione digitale

L'ago della bilancia per conferire maggiore uniformità alle riflessioni sulla conservazione digitale su scala europea, potrebbe essere costituito da un Regolamento europeo per ora assente, poiché – si vedrà nella parte IV le legislazioni nazionali percepiscono questo tema in maniera diversificata: la normativa comunitaria non contempla, attualmente, un provvedimento unitario in materia di conservazione digitale che fornisca il filo conduttore per la realizzazione di provvedimenti nazionali uniformi, progetti, iniziative e standard. Nonostante ciò, non mancano i vincoli applicabili all'ambito della *digital preservation*: vi sono limiti mandatori imposti da altri Regolamenti e direttive che, in maniera diretta o tangenziale, stabiliscono un perimetro importante.

Se, infatti, con il Regolamento eIDAS[1] si è arrivati ad avere parametri omogenei per la diffusione delle identità, delle firme, dei recapiti e dei riferimenti temporali digitali, aprendo di fatto la strada per una gestione uniforme di questi ultimi a livello europeo, manca l'equivalente riferimento per la conservazione digitale. Si può imputare questa carenza a diverse circostanze[2]: in primo luogo, si deve tenere conto della soggettività del trattamento della documentazione negli ordinamenti dei singoli Stati; in secondo luogo, è da considerare che il fatto che questi documenti costituiscano la memoria storica di ciascun Paese implica l'intersezione con esigenze di salvaguardia del patrimonio culturale; vi è poi l'aspetto connesso alla diversità del *background* archivistico delle singole realtà; infine, va ricordato che la normativa comunitaria, sebbene il range tematico sia ovviamente ampio, si concentra principalmente sugli obiettivi di tutela degli utenti e dei consumatori e di creazione di un mercato unico[3].

Dunque, ciò che, per il momento, è da ricercare e rilevare ai fini di ricostruire il quadro normativo che impatta sulla progettazione, impostazione e realizzazione di sistemi di

[1] Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (da qui innanzi eIDAS).

[2] I fattori che determinano le difficoltà di giungere a un Regolamento sulla conservazione digitali risultano evidenti dalle descrizioni dei contesti affrontata nella Parte III.

[3] Questi aspetti risalteranno tanto nell'esposizione dei casi di studio nella la Parte III quanto nelle considerazioni all'interno della Parte IV.

conservazione digitale è l'insieme di disposizioni, contenute in diversi regolamenti e direttive della Comunità Europea, che in vario modo delimitano le modalità e le caratteristiche che condizionano i legislatori nazionali nello stabilire regole o che, in assenza di queste, comunque stabiliscono dei termini mandatori entro cui è necessario operare per la definizione di sistemi di conservazione[4].

eIDAS e le novità della *Proposal for a Regulation of the European parliament and of the Council amending Regulation (EU) No 910/2014*

Si è già menzionato il Regolamento eIDAS, sul quale è interessante l'approfondimento non solo per il contenuto della norma vigente, ma anche per l'attuale proposta di modifica che la riguarda: questo descrive i vincoli per le modalità di implementazione dei regimi di identificazione elettronica, per la generazione di firme elettroniche semplici, avanzate e qualificate, per la validazione temporale elettronica, per il recapito elettronico e per l'autenticazione dei siti web, nonché le caratteristiche che un prestatore di tali servizi deve possedere perché questi vengano considerati fiduciari qualificati[5].

L'articolo che impatta sulla conservazione digitale è il 34 *Servizio di conservazione qualificato delle firme elettroniche qualificate*:

> 1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica. 2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate rispondano a dette norme[6].

[4] Si premette che la normativa comunitaria si cita in italiano, in quanto la traduzione nelle lingue dei Paesi UE è prevista istituzionalmente dalla Comunità Europea stessa.

[5] Su eIDAS si vedano G. Manca, *Conservazione digitale, la qualifica eIDAS per gli operatori: ecco come funziona*, «Agenda digitale», 09 febbraio 2021, disponibile online al sito <https://www.agendadigitale.eu/documenti/conservazione-digitale-la-qualifica-eidas-per-gli-operatori-ecco-come-funziona/>; G. Manca, *Gli standard di conservazione con il regolamento eIDAS: che c'è da sapere*, «Agenda digitale», 23 gennaio 2019, disponibile online al sito <https://www.agendadigitale.eu/documenti/gli-standard-di-conservazione-con-il-regolamento-eidas-che-ce-da-sapere/>.

[6] Art. 34 Reg. UE 910/2014.

L'articolo 40 *Convalida e conservazione dei sigilli elettronici qualificati* applica le stesse disposizioni a tale tipologia di mezzi di autenticazione[7].

Le norme richiamate da questi articoli, insieme alla conformità ai requisiti dei servizi fiduciari, corrispondono a ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*, ETSI TS 119 511 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust services providers providing long-term preservation of digital signatures or general data using digital signature techniques* e alle certificazioni ISO 9001 e ISO 27001[8].

Come si è già accennato, attualmente è in consultazione la proposta di modifica al Regolamento eIDAS[9]: questa prevede un'aggiunta importante per i servizi di conservazione digitale[10], che porrebbe parzialmente rimedio all'assenza di un regolamento specifico in materia, attraverso l'integrazione di questo provvedimento già esistente e l'equiparazione dei *long-term archiving services* ai *qualified services* già inclusi in eIDAS. Il Considerando (33) del documento specifica che è necessario fornire un quadro giuridico comunitario per il riconoscimento transfrontaliero dei servizi di archiviazione elettronica qualificati (anche al fine di aprire nuove opportunità di mercato), in quanto gran parte degli stati membri possiede già normativa di settore per la conservazione a lungo termine dei documenti elettronici[11]. Dunque, vengono introdotte le definizioni di 'archiviazione elettronica', ovvero un «un servizio che consente la ricezione, la conservazione, la cancellazione e la trasmissione di dati o documenti elettronici al fine di garantire l'integrità, l'esattezza dell'origine e le caratteristiche giuridiche di tali dati o documenti per tutto il periodo di conservazione» e

[7] Art. 40 Reg. UE 910/2014 « Gli articoli 32, 33 e 34 si applicano *mutatis mutandis* alla convalida e alla conservazione dei sigilli elettronici qualificati».

[8] Su questi standard si veda il capitolo II.3.

[9] La proposta di modifica al Regolamento eIDAS è consultabile al link <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281>.

[10] Si veda, in proposito, G. Manca, *Nuovo regolamento eIDAS, ecco come cambia l'archiviazione elettronica*, «Agenda Digitale», 7 settembre 2021, disponibile online al sito <https://www.agendadigitale.eu/documenti/nuovo-regolamento-eidas-ecco-come-cambia-larchiviazione-elettronica/>.

[11] Considerando (33) Proposta di modifica al Regolamento eIDAS «Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione digitale sicura e affidabile al fine di consentire la conservazione a lungo termine di documenti elettronici e per i servizi fiduciari associati. Al fine di garantire la certezza del diritto e la fiducia è fondamentale fornire un quadro giuridico che agevoli il riconoscimento transfrontaliero dei servizi di archiviazione elettronica qualificati. Tale quadro potrebbe inoltre aprire nuove opportunità di mercato per i prestatori di servizi fiduciari dell'Unione.

'servizio di archiviazione elettronica qualificato', per il quale si specifica che debba soddisfare i requisiti dell'articolo 45-octies[12], il quale, inserito in una sezione apposita per i servizi qualificati di archiviazione elettronica, recita:

> Un servizio di archiviazione elettronica qualificato per documenti elettronici può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità del documento elettronico oltre il periodo di validità tecnologica. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce i numeri di riferimento delle norme applicabili ai servizi di archiviazione elettronica[13].

Il *GDPR* e il Regolamento UE sulla libera circolazione dei dati non personali

Il tema del mantenimento dell'autenticità e dell'integrità dei *records* apre la strada alla menzione di altri due regolamenti che riguardano, più da vicino, i dati contenuti nei documenti e negli archivi: il GDPR[14] e il Regolamento UE 2018/1807 sulla libera circolazione dei dati non personali[15].

Sul GDPR[16] va premesso che, essendo una norma concepita per la salvaguardia dei dati personali del consumatore, propende verso la tenuta per il minor tempo possibile di questo tipo di informazioni e, di conseguenza, non comprende specifiche indicazioni riguardo alla conservazione a lungo termine[17]. Questo principio di base della minimizzazione dei dati è apparentemente in contrasto con la tenuta permanente dei documenti, così come il diritto garantito agli interessati di chiedere la distruzione o la rettifica dei propri dati personali, ma, allo stesso tempo il GDPR non pone vincoli e impedimenti per gli aspetti connessi a queste

[12] Art. 3 *Definizioni* Proposta di modifica al Regolamento eIDAS.

[13] Art. 45-octies *Servizi di archiviazione elettronica qualificati* Proposta di modifica al Regolamento eIDAS. Le considerazioni relative alle modifiche menzionate verranno discusse nel capitolo IV.1.

[14] 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* (GDPR).

[15] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre *2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.*

[16] Sul GDPR si veda S. Calzolaio, *Protezione dei dati personali*, in Raffaele Bifulco – Alfonso Celotto – Marco Olivetti (a cura di) *DIGESTO delle Discipline Pubblicistiche*, Milano, Wolters Kluwer Italia, 2017, pp. 594-635.

[17] Considerando (39) GDPR «I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario».

attività ‘postume’ che interessano la consultazione di questi dati per l’interesse pubblico e per la ricerca e scopi di utilizzo non strettamente connessi al trattamento.

Sono tuttavia indicati due obblighi che determinano conseguenze per la formalizzazione dei rapporti per la fornitura di un servizio di conservazione: il primo riguarda la necessità della nomina a responsabile esterno del trattamento dei dati di soggetti che si trovano nella condizione di custodire documentazione contenente tali dati per conto di terzi. Questi infatti, titolari del trattamento[18], sono tenuti in tale contingenza a delegare l’attività a un responsabile del trattamento che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR e garantisca la tutela dei diritti dell’interessato: il Regolamento, in proposito, vincola il rapporto tra le due parti a un contratto che stipuli la materia disciplinata e la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento; deve prevedere anche che il responsabile tratti i dati personali soltanto su istruzione documentata del titolare del trattamento (anche in caso di trasferimento di dati personali verso un paese terzo o un’organizzazione internazionale), che garantisca l’impegno e l’obbligo alla riservatezza delle persone autorizzate al trattamento dei dati personali, che assista il titolare nel rispetto degli obblighi, che su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e, infine, che metta a disposizione le evidenze necessarie a dimostrare l’adempimento dei doveri[19].

In caso, inoltre, il responsabile del trattamento ricorra a un altro responsabile del trattamento per l’esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altra figura sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati

[18] Art. 4 c. 7 GDPR « titolare del trattamento: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell’Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri».

[19] Art. 28 c.1-3 GDPR.

contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento[20].

Il secondo obbligo, connesso al precedente, prevede la nomina da parte del titolare al trattamento o da parte del responsabile della figura del *Data Protection Officer,* ovvero una figura di supporto e risoluzione esperta nel vaglio delle questioni inerenti al trattamento dei dati personali[21].

Il GDPR, inoltre, nell'ottica di una libera circolazione dei dati, non fa menzione del luogo di conservazione di questo tipo di dati: non stabilisce né un vincolo di collocazione in territorio nazionale, né nega la possibilità di porli in altro Stato UE, lasciando di fatto a discrezione del singolo Paese la decisione su eventuali eccezioni al principio di libera circolazione[22].

Il Regolamento UE 2018/1807, invece, è stato emanato con l'esplicita finalità di impedire che siano imposte limitazioni di questo tipo, in quanto «gli obblighi di localizzazione dei dati costituiscono un chiaro ostacolo alla libera prestazione di servizi di trattamento di dati in tutta l'Unione e al mercato interno[23]»: si considera, infatti, che

> la libera circolazione dei dati nell'Unione svolgerà un ruolo importante nel raggiungere una crescita e un'innovazione basate sui dati. Come le imprese e i consumatori, anche le autorità pubbliche e gli organismi di diritto pubblico degli Stati membri traggono beneficio da una maggiore libertà di scelta per quanto riguarda i fornitori di servizi basati sui dati, da prezzi più competitivi e da una maggiore efficienza nella prestazione di servizi ai cittadini. Considerata la grande quantità di dati che le autorità e gli organismi di diritto pubblico gestiscono, è

[20] Art. 28 c. 4 GDPR. Questo specifica che, in caso di inadempimento degli obblighi, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

[21] Art. 37 GDPR «1.Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10».

[22] Vi è, per giunta, anche un capo dedicato al trasferimento dei dati in paesi terzi: nel Capo V *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali* (artt. 44-50 GDPR) si stabilisce che sia consentito effettuare tali movimenti, soltanto alle condizioni del Regolamento stesso.

[23] Considerando (18) Reg. UE 2018/1807.

> estremamente importante che essi diano l'esempio avvalendosi di servizi di trattamento dei dati e si astengano dall'applicare restrizioni alla localizzazione dei dati quando utilizzano i servizi di trattamento dei dati[24].

Dunque, non solo viene vietata questa circostanza[25], ma viene anche affermato che la Commissione si incarica di facilitare l'elaborazione di codici di autoregolamentazione a livello dell'Unione, per contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità e nell'ambito della quale si tenga debitamente conto degli standard aperti, considerando le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati e applicando degli approcci in materia di sistemi di certificazione che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali, basandosi su norme consolidate a livello nazionale o internazionale che agevolano la comparabilità di tali prodotti e servizi[26].

Si noti, in ogni caso, che la consultazione dei dati da parte delle autorità viene concessa sia da questo Regolamento[27], sia dal Regolamento (UE) 2017/2394[28]: quest'ultimo conferisce specificatamente la facoltà alle autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori «il potere di accesso ai documenti, ai dati o alle informazioni pertinenti relativi a un'infrazione di cui al presente regolamento, in qualsiasi forma o formato e indipendentemente dal loro supporto di conservazione o dal luogo in cui essi sono conservati[29]» e

> il potere di esigere che qualsiasi autorità pubblica, organismo o agenzia del loro Stato membro o qualsiasi persona fisica o giuridica fornisca informazioni, dati o documenti pertinenti in

[24] Considerando (13) Reg. UE 2018/1807.

[25] Art. 4 comma 1 Reg. UE 2018/1807 «Gli obblighi di localizzazione dei dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità».

[26] Art. 6 Reg. UE 2018/1807.

[27] Art. 5 comma 1 Reg. UE 2018/1807 « Il presente regolamento non pregiudica la facoltà delle autorità competenti di chiedere od ottenere l'accesso a dati ai fini dell'esercizio delle loro funzioni ufficiali conformemente al diritto dell'Unione o nazionale. L'accesso ai dati da parte delle autorità competenti non può essere rifiutato per il fatto che i dati sono trattati in un altro Stato membro».

[28] Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio, del 12 dicembre 2017*, sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il regolamento (CE) n. 2006/2004*.

[29] Art. 9 c. 3 lett. a) Reg. (UE) 2017/2394.

qualsiasi forma o formato e indipendentemente dal loro supporto di conservazione o dal luogo in cui sono conservati, al fine di stabilire se si è verificata o si sta verificando un'infrazione di cui al presente regolamento e al fine di accertare le caratteristiche di tale infrazione, compreso tracciare i flussi finanziari e dei dati, accertare l'identità delle persone coinvolte in tali flussi, e accertare le informazioni sui conti bancari e la titolarità dei siti web[30].

Consente alle autorità, inoltre,

il potere di effettuare le necessarie ispezioni in loco, anche accedendo a locali, terreni o mezzi di trasporto utilizzati dall'operatore interessato dall'indagine nell'ambito della sua attività commerciale, industriale, artigianale o professionale, o chiedere ad altre autorità pubbliche di effettuarle per consultare, selezionare, fare o ottenere copie di informazioni, dati o documenti, a prescindere dal loro supporto di conservazione; il potere di sequestrare le informazioni, i dati o i documenti per il periodo necessario e nella misura adeguata all'espletamento dell'ispezione; il potere di chiedere a qualsiasi rappresentante o membro del personale dell'operatore interessato dall'indagine di fornire spiegazioni dei fatti, informazioni, dati o documenti relativi all'oggetto dell'indagine e registrarne le risposte; [..] il potere di acquistare beni o servizi effettuando acquisti campione, ove necessario in forma anonima, al fine di individuare infrazioni di cui al presente regolamento e raccogliere prove, compreso il potere di ispezionare, osservare, esaminare, smontare o testare beni o servizi[31].

Prescrive, riguardo alla possibilità avanzare tali richieste, la collaborazione tra le autorità competenti sul tema sia in territorio nazionale sia oltre confine[32].

I provvedimenti sulla sicurezza

È evidente come il rispetto dei regolamenti già citati si rapporti con la sicurezza dei sistemi in cui questi dati sono collocati, in particolare se questi sono forniti da soggetti terzi. La gestione degli aspetti inerenti alla sicurezza, nella sua duplice accezione fisica e logica, è normata a livello europeo in particolare da una Direttiva e un Regolamento.

In primo luogo, la Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 *recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi*

[30] Art. 9 c. 3 lett b) Reg. (UE) 2017/2394.
[31] Art. 9 c. 3 lett. c), d) Reg. (UE) 2017/2394.
[32] Art. 11-13, 15-17 Reg. (UE) 2017/2394.

informativi nell'Unione[33] include, tra i settori che rientrano nell'ambito di applicazione, le infrastrutture digitali e servizi cloud: i fornitori di tali servizi sono tenuti all'adozione di misure tecniche e *policies* organizzative, che riguardino, in particolare, la sicurezza dei sistemi e degli impianti, il trattamento degli incidenti, la gestione della continuità operativa, il monitoraggio, l'audit, i test e la conformità con le norme internazionali; inoltre, è fatto nella direttiva obbligo di notificare senza indebito ritardo gli incidenti che hanno un impatto rilevante sulla fornitura del servizio o all'autorità competente o al *Computer Security Incident Response Team* (CSIRT) nazionale[34].

Si inserisce, poi, nella scia di questa Direttiva e del già citato GDPR il Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 *relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione*[35]: scopo di tale provvedimento è delineare principi comunitari per la certificazione della sicurezza informativa dei prodotti ITC e dei servizi digitali e di consolidare le competenze dell'ENISA; ovvero l'*European Union Agency for Cybersecurity* (Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione). Le motivazioni alla base di tale finalità risiedono nel fatto che i sistemi di certificazione della sicurezza sono in capo alle nazioni comunitarie: conseguentemente, con l'obiettivo di facilitare i fornitori di servizi agli scambi internazionali, si è optato per istituire un quadro europeo che delinei lo schema entro cui costruire la valutazione per la certificazione, rendendo così quest'ultima, a prescindere dal Paese in cui è stata ottenuta, riconosciuta in tutti gli Stati membri.

Nell specifico, la prima parte del provvedimento descrive le funzioni dell'ENISA: a questa Agenzia (ora con mandato permanente) vengono aggiunti ai compiti che già possedeva di la consulenza a livello tecnico per la redazione di *policies* di sicurezza delle reti

[33] Questo provvedimento è noto anche con la denominazione Direttiva NIS (*Network and Information Security*). Si veda, in proposito, L. Tosoni, *Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto*, «Agenda Digitale», 15 gennaio 2021, disponibile online al link <https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/>.

[34] Artt. 16-17 Direttiva NIS.

[35] Questo provvedimento è noto anche con la denominazione *Cybersecurity Act*. Si veda, in proposito, L. Tosoni, , *Cibersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT,* «Agenda Digitale», 07 giugno 2019, disponibile online al link <https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/>.

e dei sistemi, gli incarichi relativi al supporto concreto alla gestione operativa degli incidenti informatici e al conferimento della certificazione di sicurezza[36].

A tal proposito, la seconda parte del *Cybersecurity Act*, riguarda la certificazione vera e propria: si conferisce all'ENISA l'incarico di comporre tali schemi di certificazione cyber security, affinché i fornitori di servizi possano presentare domanda di certificazione a specifici organismi accreditati, mentre per servizi a basso rischio prevede che si possa procedere ad una autovalutazione di conformità; viene definito che questi modelli sostituiscano quelli nazionali, le cui risultanti certificazioni, comunque, restano valide sino a scadenza[37].

Regolamentazione e accreditamento

Vi sono, infine, testi di legge che non hanno attinenza diretta con i sistemi e il trattamento del contenuto dei documenti, ma che hanno a che fare con le disposizioni di natura tecnica e operativa che i diversi Stati comunitari possono emettere a riguardo.

Innanzitutto, è in vigore la Direttiva (UE) 2015/1535 del Parlamento Europeo e del Consiglio del 9 settembre 2015 *che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*, che obbliga gli Stati membri a sottoporre i propri progetti di regole tecniche in materia alla Commissione europea, la quale ha a disposizione tre mesi di tempo per vagliare la proposta: al termine di questi, la consultazione può risultare in un'approvazione o un parere circostanziato, di cui il Paese proponente deve prendere atto e in base al quale deve modificare il proprio testo, rinviando comunque alla revisione anche il nuovo versionamento[38].

Esiste, poi, il Regolamento (CE) N. 765/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008 *che pone norme in materia di accreditamento e vigilanza del mercato per*

[36] Artt. 3-45 *Cybersecurity Act*.

[37] Artt. 46-62 *Cybersecurity Act*. A proposito degli schemi di certificazione, si veda anche L. Franchina, A. Fumagalli, L. Toccaceli, *Cyber security, certificazioni e sanzioni: come prosegue l'adeguamento alle norme Ue*, «Agenda Digitale», 32 aprile 2021, disponibile online al sito <https://www.agendadigitale.eu/sicurezza/cybersecurity-certificazioni-e-sanzioni-prosegue-ladeguamento-alle-direttive-ue/>.

[38] Artt. 4 e 6 Dir. (UE) 2015/1535.

quanto riguarda la commercializzazione dei prodotti: questo tange l'ambito della conservazione nella misura in cui si preveda una qualificazione istituzionale dei fornitori di servizi di conservazione in *outsourcing*, ottenuta mediante verifica di rispondenza a requisiti prefissati in normativa attraverso *Conformity Assessment Bodies* (organismi di valutazione di conformità)[39].

[39] Artt. 4-14 Reg. (CE) N. 765/2008.

I.3 Le iniziative, gli strumenti e i modelli condivisi a livello europeo[1]

In maniera 'parallela' rispetto alle decisioni normative esposte nel precedente capitolo, la comunità europea di studiosi, professionisti e ricercatori realizza, unendosi in associazioni e gruppi di lavoro e incontrandosi in occasioni di confronto e condivisione, attività e progetti finalizzati a disporre di *best practices* e strumenti volti a garantire la *long-term preservation* delle risorse digitali: la linea comune che emerge da queste esperienze internazionali è il tentativo di superare le criticità per la conservazione del patrimonio digitale innescate dal continuo e rapido progresso tecnologico, mettendo a disposizione esperienze effettive tarate su standard internazionali, condividendo linee guida elaborate in ambito collettivo e internazionale e sottoposte al vaglio periodico della comunità di riferimento ed elaborando strumenti *open access* perché si abbiano a disposizione *tools* diffusamente utilizzabili che garantiscano, in particolare, interoperabilità.

Associazioni e iniziative

Nell'ambito della ricerca sulla conservazione digitale esistono diverse associazioni internazionali che si occupano della diffusione di informazioni, notizie, documenti programmatici e strumenti a un'ampia e ben definita comunità di riferimento, fungendo da riferimento in ambito internazionale e favorendo la creazione di un *framework* coerente attorno alla conservazione digitale.

Tra queste, una delle più attive e longeve è l'Open Preservation Foundation[2]: istituita nel 2010, rappresenta uno degli esiti del progetto di ricerca PLANETS, finanziato dall'Unione Europea a partire dal 2006[3]. La Fondazione, attraverso un approccio collaborativo e operativo, si pone come obiettivo la diffusione e la promozione di buone pratiche di

[1] Si premette, come specificato dal titolo del capitolo, che si prendono in considerazione elementi condivisi in ambito comunitario e che rappresentano strumenti e raccomandazioni in esso ampiamente presi in considerazione e utilizzati, ma non necessariamente concepiti in questa estensione 'territoriale' di riferimento.

[2] Il sito ufficiale dell'organizzazione Open Preservation Foundation è pubblicato al link <https://openpreservation.org/>.

[3] Il progetto PLANETS (*Preservation and Long-term Access through Networked Services*), realizzato dal 2006 al 2010, aveva per oggetto la costruzione di strumenti e servizi per consentire agli archivi e alle biblioteche l'accesso a lungo termine alle proprie risorse digitali. Al termine del progetto, come mezzo per sostenere gli *output* e colmare la distanza fra sviluppatori di strumenti e professionisti della conservazione digitale, venne istituita l'Open Planets Foundation, dal 2014 Open Preservation Foundation (si veda, in proposito, la pagina <https://planets-project.eu/>).

conservazione digitale: operando come organizzazione associativa indipendente e senza fini di lucro, accoglie nella propria comunità professionisti della conservazione digitale di tutto il mondo[4]. In ottica di cooperazione e sostenibilità, produce, monitora e aggiorna linee guida, strumenti e risorse di supporto *open source* per una conservazione digitale efficace ed efficiente: l'obiettivo è consentire alle organizzazioni di valutare il proprio patrimonio digitale, effettuando valutazioni sui formati e sulle caratteristiche da mantenere, convalidare e documentare procedure ed elaborare i propri contenuti digitali secondo le logiche più appropriate per la conservazione a lungo termine.

In concreto si tratta, per i software, dell'OPF *Reference Toolset*[5], composto da quattro strumenti *open source*: questo consiste in *JHOVE*, strumento *open source* di identificazione, convalida e caratterizzazione dei formati dei file, implementato come applicazione Java e utilizzabile su qualsiasi piattaforma Unix, Windows o OSX attraverso l'installazione Java appropriata, disponibile in tre versioni: come riga di comando per l'integrazione nei flussi di lavoro di *digital preservation* da parte di tecnici, come interfaccia *desktop GUI* per gli utenti generici e come API JHOVE per gli sviluppatori che intendono incorporare questa soluzione nei progetti; *veraPDF*, ovvero un validatore PDF/A, che copre tutte le sezioni dei file con questo formato e comprende quattro componenti: un *checker* di implementazione, che convalida tutte le parti e i livelli di conformità delle specifiche PDF/A, uno delle *policies*, che consente agli utenti di implementare controlli personalizzati aggiuntivi per applicare le proprie regole oltre alle specifiche PDF/A, un reporter che elabora i risultati, producendo relazioni *human and machine readable* e un *fixer* di metadati, che ripara questi ultimi sulla base della conformità allo standard; *jpylyzer*, validatore ed estrattore di caratteristiche per le immagini JP2, formato delle immagini fisse definito nella Parte 1 dello standard di compressione delle immagini JPEG 2000[6]: analizza un file e ne esegue il contenuto

[4] La strategia, elaborata con i membri dell'associazione e consultabile al link <https://openpreservation.org/wp-content/uploads/public/OPF_Strategy_2018.pdf>, stabilisce la posizione dell'OPF nel panorama della conservazione digitale e definisce le aree chiave di interesse; oltre a fornire una *roadmap* per il raggiungimento degli scopi prefissati, consente di misurare il successo delle azioni intraprese e di direzionare gli obiettivi futuri della Fondazione.

[5] Le risorse del *Reference Toolset* sono disponibili nel menu della sezione dedicata al link <https://openpreservation.org/products/opf-reference-toolset/>.

[6] Si tratta, nello specifico dello standard ISO/IEC 15444-1:*2019 Information technology — JPEG 2000 image coding system — Part 1: Core coding system*. Questo documento è disponibile al link <https://www.iso.org/standard/78321.html> (l'accesso è vincolato al pagamento della risorsa).

sottoponendolo a diversi test, ognuno dei quali si basa sui requisiti e sulle restrizioni definiti dallo standard, il fallimento dei quali implica la non conformità allo standard e la non validità del formato; infine, *FIDO* (*Format Identification for Digital Objects*) è una riga di comando per identificare i formati di file degli oggetti digitali: il software è scritto in Python ed è progettato per essere eseguito dalla riga di comando, utilizza il registro dei formati PRONOM[7], di cui restituisce gli identificatori da singoli file o *batch* di file.

Per quanto riguarda, invece, la documentazione prodotta a supporto della *community* ed elaborata con la collaborazione diretta di quest'ultima, l'OPF redige relazioni annuali sulle attività[8], realizza sondaggi[9] e mette a disposizione i materiali relativi a eventi e progetti.

Altrettanto importante è l'attività promossa dalla Digital Preservation Coalition[10]: questa organizzazione ha origine nel 2002, dalla collaborazione di diverse agenzie operanti nel Regno Unito e in Irlanda e ha come finalità la protezione del patrimonio digitale: questa associazione ha come obiettivo il fornire ai suoi membri e alla comunità di riferimento preparazione e strumenti per garantire l'accesso a lungo termine a contenuti e servizi digitali, per trarre valore duraturo da queste risorse, aumentando la consapevolezza delle sfide strategiche, culturali e tecnologiche che è necessario affrontare. Questi scopi sono formalizzati nel Piano Strategico per il 2018-2022[11], che prevede il coinvolgimento della comunità di riferimento, per comprendere un numero sempre crescente di enti e individui in tutti i settori e in tutti i Paesi; un'azione di *advocacy* per contesti politico-istituzionali più reattivo e meglio informato sulle criticità della conservazione digitale e per aumentare la consapevolezza sulle nuove opportunità create dagli *assets* digitali; la formazione di figure professionali competenti e preparate; la diffusione e l'elaborazione di buone pratiche e standard, per il mantenimento di servizi di conservazione digitale sostenibili, resistenti all'obsolescenza e di alta qualità, attraverso lo scambio di conoscenze, il controllo della

[7] Questo registro, gestito dagli UK National Archives, è una risorsa che contiene informazioni sui formati di file, prodotti software e altri componenti tecnici necessari per supportare l'accesso a lungo termine a documenti elettronici e altri oggetti digitali <https://www.nationalarchives.gov.uk/PRONOM/Default.aspx>.

[8] I report sono consultabili al link <https://openpreservation.org/resources/annual-reports/>.

[9] I *surveys* sono disponibili al link <https://openpreservation.org/resources/surveys/>.

[10] Il sito ufficiale della Digital Preservation Coalition, in cui sono reperibili le informazioni sull'associazione, è pubblicato al link <https://www.dpconline.org/>.

[11] Lo *Strategic Plan 2018-2022* è consultabile al link <https://www.dpconline.org/docs/miscellaneous/about/1755-dpc-strategic-plan-2018-22/file>.

tecnologia, la ricerca e lo sviluppo; la garanzia, infine, di una governance stabile e focalizzata sulle esigenze della *community* designata, per disporre di una piattaforma solida e affidabile per la collaborazione all'interno e all'esterno della Coalizione.

Interessante è il catalogo di materiali e di iniziative che la DPC mette a disposizione, in parte ad accesso libero e in parte limitato ai membri, che rispecchia la natura intersettoriale e trasversale dell'organizzazione stessa[12]: le sezioni in cui è suddiviso sono *Discover Good Practice*, *Implement digital preservation*, *Champion Digital Preservation*, *Train your staff*, *Collaborative Projects*. Vi si trova distribuito l'insieme di risorse a supporto delle attività di conservazione digitale che va dalla semplice guida introduttiva per *beginners* alla conservazione digitale *What is digital preservation?* alla realizzazione di *toolkit* per casi d'uso specifici, come l'*Electronic Document and Records Management Systems (EDRMS) Preservation Toolkit*, realizzato dalla DRMS Preservation Task Force, istituita dalla DPC a seguito di un progetto con la Nuclear Decommissioning Authority.

Queste due associazioni sono promotrici di seminari e conferenze che trattano diversi temi inerenti alla *digital preservation*: alcuni esempi recenti sono costituiti dall'*Open Preservation Foundation Conference* (OPFCON 2020)[13], ha avuto luogo in occasione del decimo anniversario dell'associazione e dai webinar DPC finalizzati a illustrare *showcases* e prodotti[14].

Inoltre, costituiscono parte attiva dell'organizzazione della maggiore evento sul tema a livello mondiale, iPRES – *International Conference on Digital Preservation*[15]: iPRES è una serie di conferenze internazionali sulla *digital preservation* che ha avuto inizio nel 2004 a Beijing su iniziativa della Chinese Academy of Science (CAS) e dell'Electronic Information

[12] La raccolta è pubblicata al link <https://www.dpconline.org/digipres>.

[13] L'evento si è svolto dal 9 al 10 giugno 2020, l'agenda è disponibile al link <https://openpreservation.org/wp-content/uploads/public/resources/opfcon/2020/OPFCON_Agenda_v05_200604.pdf>.

[14] Si citano, a titolo di esempio, gli episodi su Arkivum e LIBNOVA: l'elenco dei webinar è consultabile nella sezione *Events* del sito della DPC al link <https://www.dpconline.org/events>.

[15] Su iPRES si vedano il sito dell'iniziativa pubblicato al link <https://ipres-conference.org/>; F. Marti, *La conservazione digitale in ambito internazionale. Alcune riflessioni da ipres 2019* (Amsterdam, 16-20 settembre 2019), «AIDAinformazioni. Rivista di Scienze dell'Informazione», 38 (2020), 1, pp. 133-149; *handbook* di iPRES 2021, disponibile al link <https://files.sciconf.cn/upload/file/20211016/20211016013142_82398.pdf>.

for Libraries (eIFL). Ospitata ogni anno da una nazione differente[16], ha avuto dal 19 al 22 ottobre 2021 la diciassettesima e ultima edizione a Pechino ad opera del comitato organizzativo della National Science Library della Chinese Academy of Sciences[17].

Ogni singolo evento annuale comprende workshop, sessioni intensive di *panels* ed esperienze interattive, tra cui la visita ad alcune delle istituzioni specializzate in conservazione del patrimonio culturale digitale e digitalizzato della località ospitante: il tema scelto, differente per ogni occasione, ha comunque al centro focus riguardanti la collaborazione tra le diverse tipologie di soggetti coinvolti nelle procedure di conservazione, ovvero come renderla più efficace e interpretarne l'impatto sociale (in che modo le tecnologie digitali stanno trasformando il rapporto tra soggetti produttori e istituzioni custodi di memoria e beni culturali); la costruzione di competenze e comunità, finalizzate alla formazione e alla preparazione per i futuri professionisti della conservazione digitale, con riferimento allo sviluppo della letteratura di settore; la progettazione e la realizzazione di una conservazione digitale sostenibile, ovvero in che modo la pianificazione e programmazione di quest'ultima si sviluppano e maturano nel tempo; quali sono i modelli economici e aziendali che possono massimizzare la resa dei processi di conservazione digitale; come promuovere i programmi di conservazione e adeguarli al proprio contesto istituzionale e a quello più ampio della normativa nazionale e internazionale; l'esplorazione di nuovi orizzonti nell'ambito delle tecnologie e delle *mission*, ovvero la valutazione dell'impatto della conservazione digitale sugli scopi istituzionali degli enti, delle comunità e, più in generale, delle nazioni; come si percepisce l'effetto degli sviluppi politici sui programmi di conservazione digitale; qual è il momento opportuno per il rinnovamento degli standard; come si può preservare con successo documentazione riservata a lungo termine e come raggiungere un equilibrio tra condivisione dei dati e privacy; quali gruppi sociali non sono rappresentati negli archivi digitali o sono impossibilitati a salvaguardare il proprio retaggio culturale sotto forma di documentazione archivistica; l'avanguardia delle infrastrutture

[16] Le edizioni dal 2005 al 2019 hanno avuto luogo, rispettivamente, a Göttingen (Germania, 2005), Ithaca (NY, USA, 2006), Beijing (Cina, 2007), Londra (United Kingdom, 2008), San Francisco (CA, USA, 2009), Vienna (Austria, 2010), Singapore (2011), Toronto (Canada, 2012), Lisbona (Portogallo, 2013), Melbourne (Australia, 2014), Chapel Hill (North Carolina, USA, 2015), Berna (Svizzera, 2016), Kyoto (Giappone, 2017), Boston (Massachusetts, USA, 2018), Amsterdam (Olanda, 2019). L'edizione 2020, che doveva svolgersi a Beijing, è stata rimandata al 2021.

[17] Il sito ufficiale dell'edizione 2021 è pubblicato al link < http://ipres2020.cn/1>.

tecniche e la loro implementazione (in particolare, le principali innovazioni degli strumenti di conservazione digitale e delle soluzioni di archiviazione); come è possibile adattare gli strumenti e le strategie di conservazione digitale esistenti per affrontare le innovazioni; quali sono i più recenti progressi nella gestione, identificazione e migrazione dei formati dei file e come garantire l'autenticità e la custodia sicura dei documenti digitali.

Offrono, a riguardo, i propri contributi relatori e partecipanti provenienti da tutti i continenti e da diverse tipologie di istituzioni: si citano a titolo esemplificativo – dalle ultime due edizioni – gli interventi di David Giaretta, Lisa LaPlant, Jamie Shiers, Jessica Tieman, Irfan Zuberi e Maureen Pennock, rispettivamente afferenti a Primary Trustworthy Authorisation Body Ltd, Government Publishing Office (USA), CERN, Government Publishing Office (USA), Indira Gandhi National Centre for the Arts e British Library, sulla certificazione ISO 16363[18]; di Jeanne Kramer-Smyth, Montserrat Canela e Ineke Deserno, rispettivamente da World Bank Group, UNHCR, NATO sulla pianificazione dei processi di conservazione delle istituzioni attive su scala mondiale[19]; di Oya Y. Riege, Michael Boock, Lindsay McCormack e Nick Ruest da Ithaka S+R (USA), Oregon State University, University of Oxford e York University, sull'implementazione *in house* di un'infrastruttura di conservazione e, infine, di Trevor Owens, Andrea Goethals, Jeffrey van der Hoeven, Lisandro Pablo Olivares, Paul Wheatley e Michael Day, da Library of Congress (USA), National Library of New Zealand, National Library of the Netherlands, Biblioteca Nacional de México, Digital Preservation Coalition, (UK) e British Library sull'evoluzione dei progetti di gestione delle collezioni digitali presso le *National Libraries*[20].

Strumenti e soluzioni

[18] L. LaPlant, M. Pennock, J. Shiers, I. Zuberi, *Dawn of Digital Repository Certification Under ISO 16363 Exploring the Horizon and Beyond - Perspectives From Three Institutions*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) Proceedings of the 16th International Conference on Digital Preservation 2019, pp. 463-465, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

[19] M. Canela, I. Deserno, J. Kramer-Smyth, *The People And Processes of Digital Preservation-International organizations leveraging internal wisdom to build support for digital records*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) Proceedings of the 16th International Conference on Digital Preservation 2019, pp. 472-474, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

[20] Si veda, in proposito, il programma di iPRES 2021, consultabile al link <https://www.ipres2021.ac.cn/en/web/index/11690_965303__>; poiché la conferenza si è svolta dal 19 al 22 ottobre 2021, non sono ancora disponibili, al momento della stesura del presente elaborato, i *papers* dei singoli interventi.

Tra le principali esperienze collettive esposte nel corso di questi eventi, interessanti sono le seguenti realizzazioni: il progetto *E-ARK*, l'*Integrated Preservation Suite* della British Library e le soluzioni *Archivematica* e *Preservica*.

E-ARK (*European Archival Records and Knowledge Preservation*)[21] nasce da un progetto di ricerca internazionale sui big data finalizzato a migliorare i metodi e le tecnologie di archiviazione digitale, al fine di raggiungere coerenza su scala europea: in particolare, dal 2014 al 2017 E-ARK è stato cofinanziato dalla Commissione Europea nell'ambito dell'ICT *Policy Support Program* (PSP), specificatamente nell'area *Competitiveness and Innovation Framework Program* (CIP). Affrontando una serie di problematiche associate a tecnologie, sistemi e pratiche indipendenti e attraverso l'analisi rigorosa di set aggregati di dati, nell'ambito di E-ARK sono stati sviluppati strumenti per rendere gli archivi accessibili a livello internazionale, come specifiche tecniche, *tools* e un'infrastruttura di archiviazione integrata. In concreto, viene definito *a european "showcase" project* proprio in ragione del fatto che sono pubblicamente disponibili online tutti gli *outcomes*, tanto pratici quanto documentali: sono state prodotte linee guida sull'archiviazione elettronica paneuropea come parte dell'infrastruttura elettronica dell'UE[22], prodotti tecnici e operativi *open access* (soluzioni di acquisizione e accesso, servizi, specifiche dei metadati[23]), strumenti di *data mining* per la *business intelligence*, interfacce aperte per soluzioni già esistenti, risultati di analisi normative, risultati dei progetti pilota e documenti di lavoro sulle attività di integrazione intraprese.

L'*Integrated Preservation Suite* (IPS) è una soluzione interamente sviluppata nell'ambito della British Library[24]: è un progetto che mira a raffinare le capacità di pianificazione del

[21] Le informazioni sul progetto eArk 4 all sono consultabili sul sito dedicato <https://e-ark4all.eu/>; si veda anche <http://eark-project.com/>.

[22] Un esempio di tali indicazioni è costituito dalle *E-ARK eArchiving Content Information Type Specifications*, recentemente aggiornate e consultabili sul sito della *Digital Information LifeCycle Interoperability Standards Board* (DILCIS Board) alla voce del menù *Specification* <https://dilcis.eu/specifications>.

[23] Alcuni esempi di tali strumenti sono i *Pre-Ingest Tools*, reperibili nella sezione E-ARK *tools* del sito del progetto al link <http://eark-project.com/resources/eark-tools.html>. Le altre risorse disponibili sono raccolte nelle aree *project deliverables, E-ARK general model, E-ARK architecture, presentations, E-ARK project updates, specifications, posters and images, E-ARK annual summary reports, E-ARK benefits*, al link <http://eark-project.com/resources.html>.

[24] Il progetto è illustrato in un'apposita pagina del sito istituzionale della British Library, consultabile al link < https://www.bl.uk/projects/integrated-preservation-suite>. Si veda, in proposito, anche l'intervento pubblicato da Peter May sul blog della Digital Preservation Coalition '*Integrated Preservation Suite (IPS): a*

mantenimento a lungo termine delle collezioni digitali e a contrastare l'obsolescenza tecnologica, attraverso la conservazione del software e l'acquisizione di informazioni sui formati digitali e sull'hardware.

La suite comprende diversi componenti di base che si integrano insieme: una *knowledge base*, un *software repository*, un *policy and planning repository*, una *execution platform* e un *workbench* globale *web-based*.

Il *workbench* costituisce il principale punto di accesso all'IPS, attraverso un'interfaccia utente web-based per i professionisti della conservazione digitale che attualmente prevede tre funzioni principali, ovvero la ricerca di informazioni dalla *knowledge base*, la cura dei dati qui introdotti, la creazione e la modifica dei piani di conservazione basati sul formato.

La *knowledge base* fornisce un archivio basato su grafici di informazioni tecniche su formati di file, software e ambienti relativi alla collezione digitale della Biblioteca: i dati vengono raccolti da una varietà di fonti diverse, come PRONOM[25], e aggiunti attraverso un processo volto a garantire un collegamento appropriato dei dati, mantenendone la provenienza. Questo, in combinazione con il modello di dati sottostante, consente una ricerca relazionale, che permette, ad esempio, di chiedere quale software possa essere utilizzato per la migrazione da un formato all'altro.

Il *preservation software repository* offre la capacità di preservare il software di rendering per tutti i contenuti della raccolta della British Library: l'integrazione delle informazioni di catalogazione con la Knowledge Base consente ai risultati della ricerca del *workbench* di indicare se il software è già stato acquisito nel *repository*: se si colloca questa funzione nell'ambito della pianificazione, tale integrazione tra questi componenti ha la potenzialità di facilitare la selezione di software adatto per diminuire i rischi associati ai formati.

Il *policy and planning repository* funge da deposito per le versioni approvate dei piani di conservazione, che vengono archiviate e conservate insieme al contenuto della raccolta a cui si riferiscono, in modo che si possano comprendere le scelte e le motivazioni che hanno indotto a preservare gli oggetti in tale modalità. Inoltre, il *repository* viene utilizzato anche

scalable preservation planning toolset for diverse digital collections', consultabile al link <https://www.dpconline.org/blog/integrated-preservation-suite>.

[25] Si veda, in proposito, la nota 7.

per altra documentazione, come le valutazioni sui formati, i profili di raccolta e i materiali formativi.

L'*execution platform*, infine, consente di effettuare dei test per procedere con la l'analisi dell'approccio da adottare per sviluppare il piano di conservazione: è possibile, ad esempio, testare software di migrazione di formati diversi, al fine di selezionare il più appropriato; tale risultato è ottenuto attraverso gli script eseguibili su un campione di contenuto nella piattaforma di esecuzione, utilizzando lo strumento conservato nel s*oftware repository*. Questi script e risultati vengono referenziati e collocati nel piano di conservazione, in modo da disporre di una registrazione delle sperimentazioni che hanno avuto luogo.

Archivematica è un software *open-source* finalizzato alla conservazione a lungo termine di contenuti digitali autentici e affidabili[26]: un'applicazione basata su OAIS, che consente agli utenti di gestire gli oggetti digitali dalla fase di *ingest* a quella di accesso, con la possibilità di monitorare e controllare i servizi attraverso un *dashboard web-based*. La piattaforma utilizza anche gli standard METS, PREMIS e Dublin Core, per produrre AIP indipendenti dal sistema[27]. È personalizzabile in diversi aspetti, compresa l'identificazione dei formati, l'estrazione dei pacchetti e l'aggiunta di *policy* nazionali; si può gestire anche l'archiviazione stessa degli oggetti digitali, comprese le opzioni di spostamento di posizione e di eliminazione attraverso un processo articolato in due fasi, che richiede una giustificazione e un'approvazione per la cancellazione di un AIP archiviato.

Il codice Archivematica è rilasciato con GNU *Affero General Public License* (A-GPL 3.0)[28], disponibile gratuitamente, e anche la documentazione è rilasciata sotto licenza *Creative Commons Share-alike*[29]: questo consente trasparenza e possibilità di modifica,

[26] Le informazioni sul software Archivematica sono consultabili sul sito dedicato <https://www.archivematica.org/en/>; per approfondimenti applicativi, si vedano A. Blewer, S. Romkey, S. Ross, *Archivematica as a Case Study for Sustained Digital Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 126-133, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>; M. Goodchild, G. Hurley, *Integrating Dataverse and Archivematica for Research Data Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 234-244, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

[27] Si veda, su questi standard e il riferimento all'AIP (*Archival Information Package*), il paragrafo *Standard e raccomandazioni internazionali*.

[28] <https://www.gnu.org/licenses/agpl-3.0.en.html>.

[29] <https://creativecommons.org/licenses/by-sa/4.0/>.

miglioramento e diffusione, essendo il software sviluppato anche con finalità di integrazione rispetto a prodotti di terze parti.

L'approccio adottato è di flessibilità e personalizzazione: l'utente ha il controllo, ad esempio, sulle scelte sugli strumenti di identificazione del formato, sull'esame dei contenuti per informazioni private e personali, l'estrazione dei contenuti dei pacchetti e delle immagini e la trascrizione dei contenuti; possono anche pre-configurare la maggior parte di queste opzioni per un ingest senza interruzioni sia in fase di archiviazione sia di accesso. Archivematica prevede diversi *workflow* per il versamento: importazione di metadati e documentazione di trasmissione, acquisizione di cartelle compresse e decompresse, elaborazione di immagini digitali, predisposizione SIP[30], normalizzazione manuale e gestione di set di dati. A proposito dei formati, nel *Format Policy Registry* (FPR), peraltro integrato con PRONOM[31], Archivematica implementa le sue *policies* predefinite sui formati, basate sull'analisi delle loro caratteristiche significative: l'FPR offre una struttura modificabile e flessibile per l'identificazione del formato, l'estrazione dei pacchetti, la trascrizione e la normalizzazione per la conservazione e l'accesso; gli utilizzatori del software possono aggiornare strumenti, regole e controlli nel proprio FPR locale dal server FPR gestito da *Artefactual Systems, Inc.*.

Per quanto riguarda la ricerca delle risorse e la gestione delle stesse, è possibile effettuare la ricerca nei backlog e nell'archivio dalla *web-based dashboard,* per scaricare gli AIP archiviati come pacchetti completi, singoli oggetti o ogni pacchetto in un AIC[32]. È previsto anche uno *Storage Service,* che include un processo di eliminazione in due fasi che richiede giustificazione e approvazione per l'eliminazione di un AIP archiviato.

Infine, per migliorare i propri prodotti, Archivematica si appoggia ai *feedback* della *community* di riferimento, che a sua volta può monitorare gli sviluppi della piattaforma: effettua riunioni di gruppi di utenti, formazione e workshop e accordi di installazione e servizio forniti da *Artefactual Systems, Inc.*; gli analisti di quest'ultimo gruppo

[30] *Submission Information Package*; si veda, per la terminologia OAIS, il paragrafo *Standard e raccomandazioni internazionali*.

[31] Si veda, in proposito, la nota 7.

[32] *Archival Information Packages* e *Archival Information Collection.* si veda, per la terminologia OAIS, il paragrafo *Standard e raccomandazioni internazionali*.

contribuiscono attivamente a ricerche e conferenze in cui vengono affrontate le sfide della conservazione digitale.

Preservica, infine, è il software di conservazione sviluppato dall'omonima società inglese che fa convergere le necessità di conservazione digitale a lungo termine in un'unica piattaforma integrata, basata sul modello OAIS: mantiene i contenuti in modo sicuro, garantisce che possano essere ricercati e che siano affidabili, fornisce un accesso immediato e sicuro e aggiorna automaticamente i file in formati adatti al superamento dell'obsolescenza[33]. Lo sviluppo dello strumento nasce nell'ambito del *National Archives* britannici, che, tra il 2003 e il 2007, hanno deciso di affidare a una società terza lo sviluppo di un software che si potesse occupare della conservazione dei documenti pubblici, dal momento del versamento a quello della tenuta permanente.

La piattaforma implementata consente di accedere i documenti versati tramite ricerca *full-text*, garantendo il recupero di documenti autentici: si possono visualizzare le risorse originali e tutte le copie in un'unica visualizzazione, che comprende tutti i metadati tecnici e descrittivi (formulati attraverso l'utilizzo di standard come EAD e PREMIS). Il software è in grado di eseguire il *rendering* di formati obsoleti, senza avere a disposizione l'applicazione originale o dover scaricare il file. È attivo, dunque, il meccanismo di migrazione nei formati più recenti, tramite l'integrazione con strumenti come JHOVE.

A garanzia dell'autenticità e dell'integrità, Preservica fornisce report di revisione sulle attività di conservazione, sugli audit e sui controlli all'acquisizione e audit trail dettagliati che evidenziano la provenienza dei file; inoltre, identifica, caratterizza e fissa il checksum di tutti i file attraverso flussi di lavoro completamente automatizzati e scalabili.

Progetti, linee guida e requisiti

Vi sono, poi, prodotti dell'esperienza di gruppo di lavoro internazionali, contenenti linee di indirizzo che trattano aspetti teorici, programmatici e operativi e requisiti finalizzati all'applicazione di matrici per la certificazione di depositi digitali e alla valutazione della loro consistenza.

[33] Le informazioni sulle soluzioni Preservica sono consultabili sul sito web pubblicato al link <https://preservica.com/>.

In questo senso, importante è il contributo del progetto InterPARES (*International Research on Permanent Authentic Records in Electronic Systems*)[34]: questo, attivo dal 1999 e sviluppato in ambito canadese, mira a sviluppare le conoscenze essenziali per la conservazione a lungo termine di documenti autentici nativi digitali o tenuti in forma digitale e a fornire la base per standard, *policies*, strategie e piani d'azione in grado di garantire la longevità di tale materiale e la capacità degli utenti assicurarsi della sua autenticità. Attualmente, hanno avuto luogo quattro fasi: la prima dal 1999 al 2002, la seconda dal 2002 al 2007, la terza dal 2007 al 2012, la quarta dal 2013 al 2018.

La prima *tranche* InterPARES 1 si è focalizzata sull'autenticità dei record elettronici non più necessari al soggetto produttore per svolgere le proprie funzioni. Le risorse esaminate sono consistite principalmente in documenti testuali prodotti e mantenuti in banche dati e sistemi di gestione documentale. Questa fase ha prodotto molteplici risultati, tra cui l'elaborazione di requisiti concettuali e di metodi per la selezione e la conservazione di documenti elettronici autentici: il lavoro converge nella pubblicazione *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*[35].

InterPARES 1 si è basato sui risultati del precedente progetto di ricerca *The Preservation of the Integrity of Electronic Records*, intrapreso dai ricercatori della British Columbia University dal 1994 al 1997, che mirava a stabilire standard per la creazione di *records* elettronici affidabili e il mantenimento della loro autenticità nel corso delle loro fasi attiva e semi-attiva: InterPARES è invece improntato alla trattazione dei medesimi temi una volta che questi oggetti siano diventati inattivi e selezionati per la conservazione permanente.

Il gruppo di lavoro ha compreso ricercatori e professionisti afferenti a una varietà di discipline, come diritto, storia, informatica, ingegneria e scienze dell'informazione col coordinamento, per i concetti chiave e le metodologie del progetto, di figure operanti nel campo dell'archivistica e della diplomatica. Hanno contribuito alla realizzazione di

[34] Su InterPARES si veda il sito istituzionale del progetto pubblicato al link <http://www.interpares.org/welcome.cfm>.

[35] L. Duranti (a cura di), *The InterPARES project: the long-term preservation of authentic electronic records: the findings of the InterPARES Project*, 2001, disponibile online al sito <http://www.interpares.org/book/index.cfm>.

InterPARES università, istituzioni archivistiche, imprese e aziende canadesi, statunitensi, inglesi, australiani, cinesi, francesi, irlandesi, italiane, olandesi, svedesi e portoghesi.

La seconda fase dell'iniziativa, InterPARES 2 *Experiential, Interactive, Dynamic Records*, finanziata principalmante dal programma *Major Collaborative Research Initiatives* (MCRI) del *Canada's Social Sciences and Humanities Research Council* e il *National Historical Publications and Records Commission e National Science Foundation* degli Stati Uniti. Gli obiettivi del progetto si sono ampliati per articolare i concetti, i principi, i criteri e i metodi che possono garantire la creazione e il mantenimento a lungo termine di documenti accurati e affidabili, prodotti nel contesto di attività artistiche, scientifiche e governative realizzate utilizzando anche tecnologie dinamiche. Anche in questo caso, il team è composto di figure multidisciplinari, al fine di riflettere tanto sugli aspetti connessi al *record* come bene culturale quanto sulle necessità giuridiche legate al loro valore per gli adempimenti agli obblighi di legge e per lo svolgimento di procedimenti: archivisti, figure professionali operanti nel campo dell'arte, scienziati, specialisti del settore e rappresentanti dei governi di tutto il mondo hanno lavorato insieme per affrontare la sfida rappresentata dalla manipolabilità e dall'incompatibilità dei sistemi digitali.

InterPARES 3, fase dal titolo *Theoretical Elaborations into Archival Management (TEAM): Implementing the theory of preservation of authentic records in digital systems in small and medium-sized archival organizations*, ha impostato le attività sulla base di diversi team regionali, nazionali e internazionali: hanno partecipato a questa fase 'squadre' di figure provenienti da Africa, Brasile, Canada, Catalogna, Cina, Colombia, Italia, Corea, Malesia, Messico, Norvegia e Turchia. La direzione del Progetto è stata finanziata dalla sovvenzione Community-University Research Alliances (CURA) del Canada's Social Sciences and Humanities Research Council.

Questo progetto ha tradotto la teoria e i metodi di conservazione digitale sviluppati precedentemente da InterPARES e altre iniziative di ricerca in piani d'azione concreti per collezioni di documenti tenuti in archivi e spazi di archiviazione all'interno di organizzazioni dotate di risorse limitate. I punti di interesse specifici hanno riguardato le modalità di implementazione dei principi e dei modelli in archivi e depositi di piccole e medie dimensioni, allo scopo di costruire pratiche efficaci, i fattori di che determinano come mettere

in pratica le strategie appropriate agli insiemi di *records* nel proprio contesto e le competenze richieste ai professionisti per condurre tali operazioni. Sono stati, a tal proposito, elaborati moduli didattici per programmi di formazione interni, laboratori e curricula accademici che forniscono le competenze non solo per preservare a lungo termine il patrimonio documentale digitale, ma anche per garantire la responsabilità di organizzazioni e istituzioni sulla tutela dell'accuratezza e dell'autenticità delle informazioni elettroniche che producono.

InterPARES Trust (ITrust; 2012-2019), *continuum* ed 'epilogo' delle precedenti fasi, è una *partnership* di ricerca che comprende oltre cinquanta università e organizzazioni, nazionali e internazionali, pubbliche e private, in Nord America, America Latina, Europa, Africa, Australasia e Asia. Anche in questo caso i partecipanti coinvolti sono esperti in diversi campi: scienze archivistiche, gestione dei documenti, diplomatica, diritto, tecnologia dell'informazione, comunicazione e media, giornalismo, e-commerce, informatica sanitaria, sicurezza informatica, governance e assicurazione delle informazioni, informatica forense, ingegneria informatica e politica dell'informazione. L'obiettivo perseguito consiste nel sistematizzare quanto precedentemente prodotto e definire ulteriormente i quadri teorici e metodologici, per sviluppare politiche, procedure, regolamenti, standard e legislazioni locali, nazionali e internazionali, al fine di garantire la fiducia del pubblico fondata su prove di buona governance, una forte economia digitale e una memoria digitale persistente[36].

Circa contemporaneo a quest'ultimo stadio è APARSEN, per esteso *Alliance Permanent Access to the Records of Science in Europe Network*[37], progetto avviato nell'ambito della Commissione Europea dal 2011 al 2014 che ha lo scopo di voler dare unità ai progetti sulla conservazione digitale. Si basa sulla già consolidata *Alliance for Permanent Access*, organizzazione di membri dei principali soggetti in Europa interessati alla tenuta a lungo termine dei dati digitali: il fine condiviso è creare una visione e un quadro comune per un'infrastruttura sostenibile, che fornisca un accesso permanente alle informazioni codificate digitalmente. A questo gruppo APARSEN aggiunge una vasta gamma di altri esperti, inclusi ricercatori accademici e professionisti commerciali, nonché figure provenienti da altre

[36] I prodotti di ITrust sono consultabili sul sito web appositamente predisposto al link <https://interparestrust.org/trust>.

[37] Su APARSEN si veda il sito istituzionale del progetto pubblicato al link <http://www.alliancepermanentaccess.org/>.

organizzazioni transeuropee: è stato, dunque, creato il *Virtual Centre of Excellence* sulla conservazione digitale in Europa. I temi trattati nell'ambito del programma sono le metodologie, le tecnologie, l'accesso e, soprattutto, il riutilizzo dei dati raccolti durante l'intero ciclo di vita delle risorse, la normativa e le questioni economiche, compresi gli aspetti legati ai costi e alla governance, la figura del professionista della conservazione, per fornire le qualifiche adeguate.

Gli *outcomes* del progetto consistono in particolare in consulenze, formazione e strumenti e servizi. È stato, innanzitutto, predisposto un *framework* teorico: sono stati realizzati report e documenti sui temi di *access, usability, trust, sustainability* e *integration*[38], completato dalla realizzazione di strumenti, come l'*APARSEN's Tool Repository*, punto di accesso centrale per la ricerca di software sviluppati per la conservazione digitale; questo elenco, disposto per funzionalità e tipo di dati gestiti, consente di rintracciare gli strumenti appropriati a soddisfare le esigenze delle organizzazioni, supportate nella scelta dai test effettuati nell'ambito del profetto e dalle valutazioni e dai commenti degli utenti.

Egualmente afferente alle attività di settore promosse dalla Commissione Europea è l'antecedente CASPAR (*Cultural, Artistic and Scientific knowledge Preservation, for Access and Retrieval*[39]), sviluppato dal 2006 al 2010. Questo programma di ricerca ha prodotto una struttura di strumenti e componenti infrastrutturali per supportare la conservazione di tutti i tipi di informazioni codificate digitalmente, al fine di agevolare i produttori, i curatori e gli utenti delle risorse a sostenerne l'onere di conservazione. Gli obiettivi perseguiti dal team CASPAR hanno consistito nel migliorare le tecniche per acquisire informazioni di rappresentazione e di altra tipologia, nel progettare servizi per preservare le risorse oltre l'obsolescenza hardware e software, garantire l'affidabilità dei dati custoditi con funzionalità standard per la gestione dei diritti digitali, l'autenticazione e la qualificazione e incrementare la fruibilità e l'accessibilità dei documenti.

CASPAR ha riunito un consorzio che include importanti aziende digitali, che rappresentano competenze scientifiche, culturali e artistiche, insieme a partner commerciali e leader

[38] I materiali sono disponibili alla pagina dedicata <http://www.alliancepermanentaccess.org/index.php/about-aparsen/aparsen-deliverables/>.

[39] Su CASPAR si veda il sito istituzionale del progetto pubblicato al link <http://casparpreserves.digitalpreserve.info/>.

mondiali nel campo della conservazione delle informazioni. La *Preservation User Community* fondata da CASPAR è una rete mondiale di professionisti e organizzazioni coinvolte nella conservazione delle informazioni digitali: curatori, fornitori di servizi, istituzioni della memoria, ricercatori e creatori e utenti di risorse digitali in generale.

L'obiettivo di fornire un quadro di conservazione comune per dati eterogenei e varietà di applicazioni innovative pone le sue basi nello stabilire la metodologia di base per coprire tutti gli aspetti che interessano la tenuta degli oggetti digitali: il punto di partenza è consistito in un'ampia analisi per porre le basi per il resto del progetto. Il principio guida per la realizzazione del software CASPAR è stata l'applicazione del modello di riferimento OAIS, progettando componenti per la costruzione di servizi e soluzioni adattabili a più aree, in particolare pensate per gli enti individuati per testare il programma.

Per convalidare il lavoro di ricerca, infatti, è stata effettuata una sperimentazione con diversi tipi di informazioni digitali, in un'ampia gamma di comunità di utenti, afferenti ai settori scientifico e del patrimonio culturale. La sperimentazione è stata condotta integrando i sistemi con integrazioni all'interno di varie organizzazioni: nell'ambito dei beni culturali, attraverso l'UNESCO, si sono presi in considerazione i dati necessari per documentare, visualizzare e modellare i siti archeologici; relativamente all'arte contemporanea, si è trattata la musica, che produce oggetti altamente complessi e si basa su hardware, istruzioni e dispositivi di interazione specifici: per ricreare le performance, l'archivio deve consentire il recupero di tutti questi elementi; infine, riguardo alle informazioni scientifiche, il focus ha riguardato i *records* relativi ai dati atmosferici, raccolti con strumenti diversi ed elaborati con software in evoluzione.

Non elaborati in ambito europeo, ma comunque accolte dalla comunità, sono gli NDSA Levels of preservation (LoP)[40]: si tratta di un set di criteri valutativi a più livelli, concepito nel 2013 per i primi professionisti della conservazione o per altri soggetti incaricati allo sviluppo dei sistemi di conservazione con lo scopo di approfondire le proprie conoscenze; consiste in uno strumento di base per agevolare le organizzazioni nella riflessione sui

[40] Si veda, in proposito, l'iter di stesura che la National Digital Stewardship Alliance (NDSA) per i *Levels of Preservation*, consultabili al link <https://ndsa.org//publications/levels-of-digital-preservation/> (Marti, *La conservazione digitale in ambito internazionale* cit., p. 137).

problemi relativi ai processi di conservazione. I LoP sono organizzati in cinque aree funzionali, che il gruppo di lavoro ha definito al centro dei sistemi di conservazione digitale: *storage and geographic location, file fixity and data integrity, information security, metadata* e *file formats*. Per principio programmatico, i LoP non coprono le *policies*, il personale, o le valutazioni di rischio e di bilancio, che sono tuttavia ritenute una serie di variabili da tenere in considerazione per stabilire e delineare piani di conservazione. Il gruppo di lavoro "*Levels of Preservation Reboot Working Group"*, costituito appositamente, sta effettuando la revisione dei principi per il rilascio della versione 2.0: attraverso occasioni come iPRES, il *working group* imposta dei workshop e si avvale dei *feedback* dei partecipanti, ricorrendo al vantaggio di avere raccolti in un'unica sessione i rappresentanti di una molteplicità di situazioni e istituzioni diverse.

Di formalizzazione recente, infine, sono i *TRUST Principles for digital repositories*[41]: rilasciati il 14 maggio 2020 e risultanti da mesi di consultazione e discussione della comunità di ricerca della conservazione digitale nell'ambito della *Research Data Alliance* (RDA), sono stati sviluppati al fine di facilitare l'adozione di best practices per la gestione dei *repositories*. Anch'essi non formulati in contesto europeo, sono però in questo riconosciuti: il primo giugno 2020 la stessa Open Preservation Foundation ha accolto questo set di principi, il cui punto di forza principale risiede nell'aver acquisito l'*endorsement* di diverse istituzioni su scala mondiale[42] e, dunque, nel rappresentare un documento ampiamente condiviso: la stessa estesa diffusione e volontà di genericità, però, portano con sé il limite di tali principi, ovvero la loro superficiale definizione.

Secondo questi principi, un *repository* deve essere innanzitutto trasparente, dunque identificare e comunicare chiaramente il proprio scopo, il target di utenza, le *policies*, i termini d'uso e servizi aggiuntivi, perché lo user possa comprendere se ciò che sta consultando corrisponda alle sue necessità («Transparency. To be transparent about specific

[41] L. Dawei – J. Crabtree – I. Dillo – R.R. Downs – R. Edmunds – D. Giaretta – M. De Giusti, et al., *The TRUST Principles for Digital Repositories*, «Scientific Data», 7 (2020), 1, pp. 1-5 disponibile online al sito <https://doi.org/10.1038/s41597-020-0486-7>.

[42] Sulla promozione da parte dell'OPF dei principi TRUST si veda <https://openpreservation.org/news/trust-principles-for-trustworthy-data-repositories-endorsed-by-the-open-preservation-foundation/>; l'elenco delle altre istituzioni che supportano l'adozione dei principi è consultabile alla pagina dedicata del sito web della Research Data Alliance al link <https://www.rd-alliance.org/rda-community-effort-trust-principles-digital-repositories-0 >.

repository services and data holdings that are verifiable by publicly accessible evidence»[43]); deve dichiarare la propria responsabilità («Responsibility. To be responsible for ensuring the authenticity and integrity of data holdings and for the reliability and persistence of its service») sulla custodia dei dati, sui diritti di proprietà intellettuale dei produttori, sulla protezione dei dati sensibili e sulla sicurezza del sistema e l'integrità del suo contenuto, assicurando che i dati rimarranno accessibili nel tempo e così citati e referenziabili nelle pubblicazioni accademiche; deve incentrarsi sulla comunità designata («User focus. To ensure that the data management norms and expectations of target user communities are met»), rispondendo con rapidità ai suoi cambiamenti e fornendo la possibilità di trovare, esplorare e comprendere i dati del repository con attenzione al loro potenziale uso e riuso; deve assicurare un accesso ininterrotto, presente e futuro, fornire servizi nel tempo e implementarne di nuovi, pianificare la *risk migration*, continuità operativa, *disaster recovery* e adottare *policies* per la conservazione a lungo termine («Sustainability. To sustain services and preserve data holdings for the long-term») e, infine, tenere costantemente conto delle innovazioni tecnologiche, considerato che un *repository* dipende da interazione tra persone, processi, componenti software e hardware e servizi tecnici («Technology. To provide infrastructure and capabilities to support secure, persistent, and reliable services»).

Congiunzione tra progetti, linee guida e standard sull'affidabilità dei depositi digitali[44] è l'iniziativa CoreTrustSeal[45], avviata a partire dal 2018. Questa rappresenta una certificazione di livello base per qualsiasi *repository* si voglia sottoporre all'autovalutazione, basata sul catalogo e sulle procedure del DSA e del WDS *Core Trustworthy Data Repositories*: i requisiti riflettono le caratteristiche fondamentali di archivi affidabili ed è il culmine di uno sforzo cooperativo tra *Data Seal of Approval* (DSA) e *World Data System* (WDS), con la coordinazione della Research Data Alliance per unificare le rispettive griglie di certificazione.

[43] La citazione, come le successive in parentesi, sono tratte da L. Dawei, *The TRUST Principles* cit., p. 2.

[44] Si vedano, in proposito, i *Levels of Preservation* (*supra*) e gli standard ISO 16363 e 19616 (paragrafo *Standard e raccomandazioni internazionali*).

[45] Su CoreTrust Seal si vedano il sito istituzionale pubblicato al link <https://www.coretrustseal.org/>, S. Allegrezza, *La certificazione dei depositi digitali: il* Data Seal of Approval, «JLIS.it Italian Journal of Library, Archives and Information Science» 6 (2015), 3, pp. 39-56, disponibile online al sito <https://www.jlis.it/article/view/11332/10624>.

Il sigillo CTS, infatti, ha sostituito il DSA nel 2018. Quest'ultimo è stato realizzato nel 2008 da DANS (*Data Archiving and Networked Services*), organizzazione olandese, in seguito agli input dai propri *stakeholder* per creare una 'certificazione' che garantisse che le informazioni archiviate potessero essere accessibili, intelligibili e utilizzabili in futuro. Stesso subentro avviene nell'ambito della *WDS Regular Member Certification*: nel 2011 il WDS ha sviluppato dei criteri, basati su standard riconosciuti a livello internazionale, e una procedura trasparente e obiettiva per garantire l'affidabilità dei membri titolari e fornitori di dati in termini di autenticità, integrità, riservatezza e disponibilità di dati e servizi. Da luglio 2017, le organizzazioni che fanno domanda per la prima volta o rinnovano la propria iscrizione *WDS Regular* devono essere preventivamente certificate CoreTrustSeal.

CoreTrustSeal, amministrativamente, è strutturata come un organizzazione internazionale basata sulla comunità di riferimento, non governativa e senza scopo di lucro che promuove infrastrutture di dati sostenibili e affidabili. È un'entità legale stabilita in olanda, la cui conduzione è affidata a un Comitato per gli standard e la certificazione, composto da dodici membri eletti che rappresentano l'Assemblea dei revisori e la cui azione è supportata da WDS e DANS.

La certificazione, concepita nell'ottica della sostenibilità, presenta un costo a copertura delle spese amminstrative: è considerata il primo passo in un quadro globale per la certificazione del *repository* che include la certificazione di livello esteso (Nestor-Seal DIN 31644[46]) e la certificazione di livello formale (ISO 16363). Le aree interessate dalla certificazione sono quella organizzativa, tecnica, finanziaria e legale: la valutazione di questi settori da parte di un'autorità indipendente conferisce attestazione di sostenibilità.

È, infatti, una certificazione adeguata a istituzioni che rendono conto a *stakeholder* che necessitano politiche di dati aperti e di particolare accessibilità delle risorse: si ritiene che la conservazione delle informazioni sia una garanzia dell''investimento', attuata preservando i *records* affinché rimangano utilizzabili e significativi in futuro.

La certificazione di base prevede un processo di autovalutazione interna, che viene poi visionata dalla comunità designata, che fornisce una valutazione: in tal modo si consolida la

[46] <https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor_Siegel/siegel.html>.

qualità del sistema e si aumenta la trasparenza dei processi, sia di gestione del *repository*, sia di interazione tra revisori e candidato alla certificazione. Questo favorisce anche l'acquisizione della fiducia da parte degli utenti, che possono consultare gli esiti dell'autovalutazione, ed è utile anche se non si vuole, a prescindere, richiedere la certificazione, in quanto si procede con la revisione e il vaglio delle procedure interne, che possono essere esaminate rispetto a criteri pertinenti e aggiornate ove necessario.

Con la presentazione della domanda per la certificazione effettiva, le procedure e la documentazione sul deposito sono ulteriormente valutate da professionisti esterni, tenendo conto delle finalità e del contesto specifici; in tal modo, il *repository* acquisisce informazioni indipendenti su come può evolversi e maturare per aumentare ulteriormente la propria affidabilità. Questa, inoltre, può costituire una base per certificazioni di livello superiore, in quanto i requisiti – tutti obbligatori e sono elementi indipendenti con uguale ponderazione – sono tarati su principi e standard condivisi.

Il set di requisiti, la cui versione 2017-2019 è stata aggiornata con quella 2020-2022 – revisionata sulla base dei *feedback* della comunità –, è formato da quattro documenti: *Introduction to the CoreTrustSeal Trustworthy Data Repositories Requirements 2020–2022*, *CoreTrustSeal Trustworthy Data Repositories Requirements 2020–2022*, *CoreTrustSeal Trustworthy Data Repositories Requirements: Glossary 2020–2022* e *CoreTrustSeal Trustworthy Data Repositories Requirements: Extended Guidance 2020–2022*.

I sedici requisiti, in particolare, riguardano il mandato dell'organizzazione per conservare le informazioni nel suo dominio, il mantenimento di un modello di diritti appropriati per l'accesso e l'utilizzo dei dati, di cui monitora la *compliance*, la presenza di un *continuity plan*, la garanzia che i dati siano creati, curati, resi disponibili e utilizzati in accordo a norme etiche, l'adeguatezza delle risorse economiche e la qualità del personale coinvolto nella struttura organizzativa, la disposizione e considerazione di pareri di esperti (esterni o interni), il mantenimento dell'integrità e dell'autenticità delle risorse, l'impiego di set definiti e basati su criteri standard di dati e metadati, la documentazione di processi e procedure di gestione dell'archivio, la responsabilità e la pianificazione (documentata) della tenuta a lungo termine, la dotazione agli *user* di informazioni sulla qualità dei dati, le procedure di flusso dal versamento alla distribuzione, l'identificazione persistente del singolo *record*, la capacità di

riutilizzo nel tempo dei materiali, la consistenza e il supporto dei sistemi operativi, dei software e degli hardware impiegati e la sicurezza di strutture e infrastrutture.

In conclusione, per legare il discorso con il successivo paragrafo relativo agli standard e alle raccomandazioni internazionali, si citano i *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC[47]): la loro pubblicazione risale al 2007, a seguito delle attività di un gruppo di lavoro nell'ambito del CCSDS, con la collaborazione del *Research Libraries Group* (RLG) dell'*Online Computer Library Center* e della *National Archives and Records Administration* (NARA). I criteri sono divisi in tre aree: la prima (sezione A), riguardante le infrastrutture organizzative, contiene indicazioni sulla *governance*, la struttura organizzativa e il personale, le responsabilità procedurali e quadro politico, la sostenibilità finanziaria, i contratti, le licenze e i ruoli; la seconda (sezione B), relativa alla gestione degli oggetti digitali, include aspetti sulla fase di Ingest (acquisizione di contenuti, creazione dell'AIP[48]), la pianificazione della conservazione e la gestione delle informazioni e degli accessi; la terza (sezione C), sulle tecnologie, l'infrastruttura tecnica e la sicurezza, tratta nello specifico l'appropriatezza delle *policies* e delle implementazioni su questi temi. Ogni requisito è corredato dall'elenco delle evidenze da produrre per evidenziarne la conformità.

Standard e raccomandazioni internazionali[49]

Come già affermato, tanto i lavori delle associazioni quanto le linee guida elaborate dai diversi gruppi di lavoro raccomandano l'adozione di standard, perché si abbiano modelli di sistemi di conservazione interoperabili e che garantiscano l'autenticità e l'integrità degli oggetti a lungo termine.

Quelli di maggior rilievo su questi specifici aspetti sono ISO 14721:2012 *Space data and information transfer systems — Open archival information system (OAIS) — Reference model*[50], ISO 16363:2012 *Space data and information transfer systems — Audit and*

[47] Si veda, a riguardo, la pagina dedicata sul sito web del Center for Research Libraries al link <https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac#:~:text=The%20Trustworthy%20Repositories%20Audit%20%26%20Certification,serves%20the%20repository's%20stakeholder%20community>.

[48] Si veda la nota 27.

[49] Altri standard e raccomandazioni internazionali applicati all'ambito della conservazione digitale adottati specificatamente nel contesto italiano verranno descritti nel paragrafo II.3.

[50] ISO 14721:2012 (la cui versione è stata confermata nel 2018) è consultabile online sul sito istituzionale del Consultative Committee for Space Data Systems al link < https://public.ccsds.org/pubs/650x0m2.pdf>.

certification of trustworthy digital repositories[51] e ISO 16919:2014 *Space data and information transfer systems — Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*[52].

Lo standard OAIS descrive un modello concettuale e funzionale per realizzare archivio inteso come sistema in cui soggetti produttori, responsabili del processo di conservazione e comunità di utenti interagiscono attraverso strutture e infrastrutture che garantiscono alle risorse digitali una conservazione a lungo termine[53].

Innanzitutto, definisce l'unità base, ovvero l' *information object*, costituito dall'insieme di effettivo oggetto da sottoporre a conservazione (*data object*) e di informazioni che lo riguardano (*representation information*). Queste entità formano, a loro volta, l'*information package*, contenitore concettuale costituito da *content information* (ovvero la somma di *data object* e *representation information*) e *Preservation Description Information* (PDI), che riguardano la provenienza, il contesto, i riferimenti, la stabilità e i diritti di accesso della risorsa. Questi pacchetti sono descritti attraverso le *Description information* e identificati dalle *Packaging information.*

Lo standard approfondisce, poi, le forme in cui questi pacchetti transitano dal versamento all'interno del sistema al momento in cui devono esserne estratte ai fini della consultazione, distinguendoli in *Submission Information Package* (SIP), *Archival Information Package* (AIP) e *Dissemination Information Package* (DIP)[54]: il primo è quel pacchetto che viene inviato ad un archivio OAIS da un *Producer* (la sua forma e il suo contenuto dettagliato sono tipicamente oggetto di accordi tra il produttore e chi amministra il sistema); il secondo è costituito da uno o più SIP, una volta che questi hanno effettuato l'ingresso all'interno

[51] Lo standard (la cui versione è stata confermata nel 2017) è disponibile al link <https://www.iso.org/standard/56510.html> (l'accesso è vincolato al pagamento della risorsa).

[52] Lo standard è disponibile al link <https://www.iso.org/standard/57950.html> (l'accesso è vincolato al pagamento della risorsa).

[53] Su OAIS si vedano D. Giaretta, *Advanced Digital Preservation*, Berlino, Springer, 2011, pp. 13-30, 47-63; S. Pigliapoco, *Progetto archivio digitale. Metodologia, professionalità, sistemi,* Lucca, Civita editoriale, 2020, pp. 150-168; G. Michetti, *Il modello OAIS,* «DigItalia. Rivista del digitale nei beni culturali», III (2008), 1, disponibile online al sito <http://digitalia.sbn.it/article/view/441/281>.

[54] Nel presente elaborato si utilizzano per i contesti internazionali le sigle inglesi SIP (*Submission Information Package*), AIP (*Archival Information Package*) e DIP (*Dissemination Information Package*), per il contesto italiano le abbreviazioni tradotte PdV (Pacchetto di Versamento), PdA (Pacchetto di Archiviazione) e PdD (Pacchetto di Distribuzione).

dell'archivio ed è corredato dalle adeguate e complete *Content Information* e *Preservation Description Information*; il terzo rappresenta la risposta del sistema alle richieste di consultazione.

Esistono, poi, due particolari combinazioni per l'AIP, ovvero l'*Archival Information Unit* (AlU) e l'*Archival Information Collection* (AIC): l'AIU rappresenta il tipo usato per la funzione di conservazione delle *Content information* che non sono suddivise in altri AIP; l'AIC organizza un insieme di AIP (o AIU e altre AIC) sulla base di un legame tematico, in modo tale che si efficienti l'accesso alle risorse da parte dei *Consumer*.

Per quanto riguarda la struttura in cui si articola il sistema stesso, OAIS descrive sei differenti moduli: l'entità *Ingest*, che accetta SIP dai *Producers* o da elementi interni sotto il controllo della componente *Administration* – eseguendo il controllo di qualità –, prepara i contenuti per la conservazione e la gestione all'interno *dell'Archival storage* – generando AIP ed estraendo le PDI – e coordina gli aggiornamenti del modulo di storage e *Data Management*; l'entità *Archival storage*, che riceve gli AIP da *Ingest* e li aggiunge all'archiviazione permanente, gestendo la gerarchia di archiviazione, aggiornando i supporti su cui sono memorizzati i contenuti, eseguendo il controllo degli errori ordinari e straordinari, provvedendo al *disaster recovery* e fornendo AIP al modulo *Access* in caso di richieste; l'entità *Data Management*, che fornisce i servizi per popolare, mantenere e accedere sia alle informazioni descrittive che identificano e documentano i *records* sia ai dati amministrativi utilizzati per gestire l'archivio, amministra e aggiorna le funzioni del database, esegue interrogazioni sulle informazioni di gestione dei dati per generare risposte e produce rapporti da essi; l'entità di *Administration*, che gestisce gli accordi di versamento con i produttori, controlla questa operazione, mantiene la configurazione dell'hardware e del software del sistema, fornisce funzioni per monitorare e migliorare le operazioni dell'archivio e per inventariare, rendicontare e migrare o aggiornare i contenuti, stabilisce e mantiene gli standard e le *policies*, presta assistenza ai clienti e attiva le richieste conservate; l'entità *Preservation planning*, che controlla l'intero 'ecosistema' OAIS, fornisce raccomandazioni e piani di conservazione per assicurare che le informazioni immagazzinate rimangano accessibili e comprensibili per la comunità designata, valuta i contenuti e raccomanda periodicamente aggiornamenti e migrazioni delle informazioni, fornisce rapporti periodici di

analisi dei rischi, progetta modelli di pacchetti informativi e fornisce assistenza e revisione per specializzarli in SIPs e AIPs per specifici invii; infine, l'entità *Access*, che supporta i *Consumers* nel rintracciare l'esistenza, la descrizione, l'ubicazione e la disponibilità delle risorse conservate, consentendo la richiesta e la ricezione delle informazioni di interesse e applicando controlli per limitare l'accesso, genera e consegna i DIP.

Lo standard propone, infine, tre modelli per l'interoperabilità: i *cooperating archives* si basano su accordi tra due o più archivi, che si legano attraverso la condivisione di schemi di SIP e DIP; i *federated archives* realizzano l'interoperabilità rivolgendosi a una base comune di *Consumer*, che consultano le risorse disponendo di un interfaccia e di un catalogo comune a più archivi OAIS, i quali devono condividere la struttura dei pacchetti e i linguaggi di scambio; infine, gli *archives with shared functional areas* condividono o integrano moduli funzionali, secondo appositi accordi.

ISO 16363 e ISO 19616, anch'essi sviluppati in ambito CCSDS, hanno lo scopo, invece, di certificare l'affidabilità dei depositi[55]. Il primo nasce dalle attività del gruppo di lavoro *Mission Operations Information Management Services - Repository Audit and Certification*, finalizzata all'elaborazione di una metrica su cui basare un processo di audit e certificazione per valutare la *trustworthiness* dei *repositories* digitali, il cui ambito di applicazione si estendesse a ogni genere di deposito. Il documento si articola in cinque parti, che riguardano, rispettivamente, l'introduzione a concetti, la terminologia e il quadro di riferimento, una panoramica dei criteri di valutazione e certificazione – con la menzione delle evidenze, degli standard, delle *best practices* e dei controlli – l'infrastruttura organizzativa (compresi gli aspetti contrattuali ed economici) e il *risk management* sull'infrastruttura tecnica e la sicurezza.

Il modello funzionale di riferimento per la metrica è ISO 14721: ISO 16363 rappresenta il 'filtro' cui sottoporre le scelte di implementazione del sistema OAIS, per verificarne l'effettiva rispondenza in termini di affidabilità.

[55] Su ISO 16363 e ISO 19616 si vedano M. Guercio, *I depositi per la conservazione di archivi digitali: i requisiti di certificazione e il problema dell'autenticità*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010; M. Guercio, *La certificazione e i depositi digitali: il ruolo degli standard e delle linee guida*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 245-255, disponibile online al sito <https://journal.almamater.si/index.php/Atlanti/article/view/132/119>.

Le modalità e la griglia dei requisiti per poter svolgere l'audit sull'affidabilità del deposito sono, invece, descritte in ISO 16919: il principale scopo del documento è definire una *Recommended practice* sulla quale basare le operazioni dell'organizzazione che valuta il proprio *repository* utilizzando come riferimento ISO 16363 e fornire l'appropriata certificazione. La metrica utilizzata, insieme a quest'ultimo standard, è quella di ISO/IEC 17021[56], che fornisce i requisiti per gli organismi che effettuano audit e certificazione per diversi tipi di sistemi di gestione. Va tenuto conto, in ogni caso, che per ogni tipo di sistema saranno necessari dei requisiti specifici, come l'adozione di specifiche raccomandazioni sulla base delle quali verrà effettuato l'audit e le qualifiche che gli *auditors* dovranno possedere.

Vi sono, poi, i documenti rilasciati da ETSI, l'*European European Telecommunications Standards Institute*, organizzazione europea le cui competenze riguardano l'elaborazione di standard per il campo ITC[57]. Questi sono sempre più significativi riguardo alla conservazione digitale, poiché i servizi di *long-term archiving* stanno percorrendo la strada di inclusione tra i *qualified services* eIDAS, i quali, in relazione a diverse specifiche, hanno obbligato riferimento nelle raccomandazioni ETSI.

In primo luogo, ETSI TS 533 101-1 *Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management*[58], contiene i requisiti di sicurezza che i fornitori di servizi di conservazione dei dati devono rispettare nell'implementazione e gestione di quest'ultimo, al fine di poterne garantire l'affidabilità. Queste misure sono basate sulle indicazioni di ISO/IEC 27001, ISO/IEC 27002[59] e ETSI TS 102 573[60], adeguandole ove necessario, ma non affronta specificatamente il tema della conservazione dei documenti, che si ritiene già coperto da altre norme ISO, quali 14721 e 23081. Vi è poi una seconda parte, ETSI TS 533 101-2, delinea le modalità di valutazione per verificare la conformità alle disposizioni specificate nel primo documento.

[56] ISO/IEC 17021-1:2015 *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*.

[57] Si veda, in proposito, il sito web ufficiale dell'organizzazione, pubblicato al link <https://www.etsi.org/>.

[58] La versione ETSI TS 101 533-1 V1.3.1 (2012-04) dello standard è disponibile al link . <https://www.etsi.org/deliver/etsi_ts/101500_101599/10153301/01.03.01_60/ts_10153301v010301p.pdf>.

[59] Si veda, in proposito, il capitolo II.3.

[60] ETSI TS 102 573 *Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects*, consultabile al link <https://www.etsi.org/deliver/etsi_TS/102500_102599/102573/02.01.01_60/ts_102573v020101p.pdf>.

ETSI TS 119 511 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*[61] tratta, invece, specificatamente la politica e i requisiti di sicurezza per i fornitori di servizi fiduciari che forniscono la conservazione a lungo termine delle firme digitali e dei dati in generale, sulla base di quanto indicato in ETSI EN 319 401. In particolare, l'attenzione è sull'adempimento di quanto stabilito nel regolamento eIDAS sui servizi di conservazione qualificati per le firme elettroniche qualificate o i sigilli, ma si trattano anche le firme e i sigilli semplici e avanzati.

I casi descritti sono due: il primo riguarda il mantenimento per lunghi periodi di tempo della capacità di convalidare una firma digitale, di preservare il suo stato di validità e di avere evidenza dello stato dei dati firmati al momento del versamento in conservazione, anche se in seguito la chiave di firma viene compromessa, il certificato scade o intervengano altre manomissioni; il secondo è relativo alla disposizione di prove di esistenza degli oggetti digitali, che siano firmati o meno. Il documento comprende diverse strategie, distinte, ad esempio, dalla fornitura di *storage*, dalla sua esclusione o dall'eventualità che sia temporaneo, oppure dalla ricezione della sola firma, dei dati firmati o dei valori di *hash*: i requisiti applicabili dipendono da dalla strategia scelta dal servizio di conservazione; nel documento, vengono indicati i controlli specifici necessari per affrontare i rischi legati alle differenti situazioni.

Si cita, infine, ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*[62], proprio in relazione al potenziale cambiamento di *status* dei servizi di conservazione[63]: queste raccomandazioni identificano i requisiti generali relativi ai fornitori di servizi fiduciari (TSP) indipendentemente dal tipo di TSP, sia esso emittente di certificati (qualificato o meno), di marche temporali, di verifica della firma o altra forma di prodotto che supporta la firma elettronica. Definisce la politica requisiti sul funzionamento e le prassi di gestione dei TSP, coprendo le aree relative ai

[61] La versione ETSI TS 119 511 V1.1.1 (2019-06) dello standard è disponibile al link <https://www.etsi.org/deliver/etsi_ts/119500_119599/119511/01.01.01_60/ts_119511v010101p.pdf>.

[62] La versione dello standard ETSI EN 319 401 V2.3.1 (2021-05) è disponibile al link <https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf>.

[63] Si noti, in aggiunta, che lo standard è stato incluso nel nuovo Regolamento italiano sulla fornitura di servizi di conservazione qualificati (si veda, in proposito, il capitolo II.2).

concetti generali, agli obblighi e alle responsabilità, alla gestione dei processi e dell'operatività, alla struttura organizzativa e alla compliance normativa.

Vi sono, infine, i modelli per elaborare i corredi di metadati da associare al patrimonio conservato.

Il *Dublin Core Metadata Element Set* è un dizionario di quindici proprietà da utilizzare nella descrizione delle risorse[64]. Questi quindici elementi sono parte di un insieme più ampio di vocabolari di metadati e specifiche tecniche mantenuti dalla *Dublin Core Metadata Initiative* (DCMI), avviata nel 1995 nell'ambito della già citata OCLC: il set completo, ovvero il DCMI *Metadata Terms*, include anche set di classi di risorse (come il DCMI Type Vocabulary), schemi di codifica del vocabolario e schemi di codifica della sintassi. I termini negli strumenti DCMI possono essere utilizzati in combinazione con termini di altri vocabolari compatibili nel contesto dei profili applicativi e sulla base del DCMI *Abstract Model* (DCAM). Questa versione 'abbreviata' di quindici componenti consente di creare strutture dati per descrivere le risorse digitali e agevolarne l'accesso. A tale scopo, è stato elaborato anche il *Dublin Core Collection Application Profile*, che descrive un profilo di applicazione Dublin Core per rappresentare una collezione o un catalogo o indice, ovvero un'aggregazione di metadati relativi a una collezione.

Lo standard, nel 2009, è stato formalizzato come norma dall'International Standard Organization: le versioni attualmente confermate sono ISO 15836-1:2017 *Information and documentation — The Dublin Core metadata element set — Part 1: Core elements* e ISO 15836-2:2019 *Information and documentation — The Dublin Core metadata element set — Part 2: DCMI Properties and classes*[65].

Appositamente elaborato per definire i metadati di conservazione è il complesso di risorse realizzate nell'ambito del gruppo di lavoro PREMIS, *Preservation Metadata: Implementaton*

[64]Lo standard è disponibile al link <https://www.dublincore.org/specifications/dublin-core/dces/>. Si vedano, in proposito, le informazioni presenti nel sito web dello standard e P. Feliciati, *Gestione e conservazione di dati e metadati per gli archivi: quali standard?*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010, pp. 191-219; S. Pigliapoco, *Progetto archivio digitale* cit., p. 71.

[65] La versione ISO dello standard Dublin Core sono disponibili ai link https://www.iso.org/standard/71339.html (Parte 1) e <https://www.iso.org/standard/71341.html> (Parte 2); l'accesso è vincolato al pagamento della risorse.

strategies, attivato nel 2003 nell'ambito della stessa OCLC[66]. Si tratta, in primo luogo, del *Data Dictionary for Preservation Metadata*, ovvero un dizionario per implementare metadati di conservazione nei sistemi che supportino l'accessibilità, l'utilizzabilità, l'intellegibilità, l'autenticità e l'identità degli oggetti digitali nel contesto di conservazione, che rappresentino le informazioni che la maggior parte dei depositi di conservazione ha bisogno siano esplicitate per garantire la tenuta dei materiali a lungo termine, che siano rigorosamente definiti, supportati da linee guida per la creazione, gestione e uso, e orientati verso flussi di lavoro automatizzati, che esprimano una neutralità tecnica tale da non presupporre l'utilizzo di eventuali software. Il *Data model* PREMIS si articola in quattro entità: l'*object* è definito come unità di informazioni soggetta alla conservazione, che a sua volta è collegato all'*environment*, ovvero la tecnologia software o hardware che supporta la resa o l'esecuzione dell'oggetto (descrivibile come *Intellectual entity*, che, costituisce una delle tipologie di o*bject* con *representation file* e *bitstream*); l'*agent* è una persona, un'organizzazione, un software o un sistema associato agli eventi nel ciclo di vita di un oggetto o legato ai diritti ad esso collegati; la *rights statement,* infine, è la dichiarazione di uno o più diritti o permessi che attengono all'oggetto o all'agente. Queste entità sono gestite tenendo in considerazione le relazioni che intercorrono tra loro, che lo standard distingue in tre tipologie: strutturali, ovvero sussistenti tra i file che costituiscono una rappresentazione di un'entità intellettuale, di derivazione, quando vi sono delle modifiche nella consistenza dell'oggetto, e, infine, di dipendenza, cioè relative a componenti esterne all'oggetto che sono, però, essenziali alla sua rappresentazione.

Pur non strettamente attinente alla metadatazione per la conservazione *tout-court*, va menzionato lo standard ISO 23081, che si articola in due documenti distinti: ISO 23081-1:2017 *Information and documentation — Records management processes — Metadata for records — Part 1: Principles* e ISO 23081-2:2021 *Information and documentation —*

[66] Le versioni dello standard sono disponibili al link <https://www.loc.gov/standards/premis/>. Si vedano, in proposito, P. Caplan, *Understanding PREMIS*, Library of Congress' Network Development and Marc Standards Office, 2009, disponibile online al sito <http://www.loc.gov/standards/premis/understanding-premis-rev2017.pdf>; P. Feliciati, *I metadati nel ciclo di vita dell'archivio digitale e l'adozione del modello PREMIS nel contesto applicativo nazionale*, in Giorgetta Bonfiglio-Dosio - Stefano Pigliapoco (a cura di), *Formazione, gestione e conservazione degli archivi digitali. Il master FGCAD dell'Università degli Studi di Macerata*, Macerata, EUM, 2015, pp. 189-208; M. Guercio, *Conservare il digitale* cit., pp. 83-88; S. Pigliapoco, *Progetto archivio digitale* cit., pp. 73-76.

Metadata for managing records — Part 2: Conceptual and implementation issues[67]. Il primo è finalizzato a coprire i principi base che determinano la costruzione dei metadati di gestione dei record: questi sono applicabili ai *record* e ai relativi metadati, a tutti i processi che li riguardano, a qualsiasi sistema in cui risiedono, a qualsiasi organizzazione responsabile della loro gestione. Il secondo stabilisce un *framework* per la definizione di metadati coerenti con i principi e le considerazioni sull'applicazione contenuti in ISO 23081-1. Gli scopi perseguiti sono consentire una descrizione standardizzata dei *record* e delle entità contestuali con cui si relazionano, fornire una linea comune per agevolare l'interoperabilità dei record e delle informazioni rilevanti tra i sistemi e permettere il riutilizzo e la standardizzazione dei metadati per la gestione degli oggetti digitali nel tempo, nello spazio e tra le applicazioni (aspetto, quest'ultimo, rilevante riguardo alla conservazione digitale). Identifica, inoltre, alcuni dei nodi decisionali critici che devono essere affrontati e documentati per consentire l'implementazione dei metadati per la gestione dei *record*: questo punto riguarda le figure coinvolte nelle scelte, i percorsi di valutazione e le opzioni e i procedimenti.

Allo scopo di completare il quadro tracciato, infine, si accenna un riferimento a ISAD(G), ISAAR(CPF) e ISDIAH, elaborati nell'ambito dell'International Council on Archives: concepiti in ambito analogico e applicabili anche alle collezioni digitali, sono standard descrittivi che mirano, rispettivamente, alla rappresentazione dei fondi archivistici, dei soggetti produttori e di istituzioni detentrici di collezioni documentali.

ISAD (G), per esteso *General International Standard Archival Description*, formulato nel 1992, ha lo scopo di fornire una struttura entro cui costruire le descrizioni archivistiche. Si basa sul concetto di archivio come insieme gerarchico di componenti, la cui rappresentazione va articolata su più livelli dal generale al particolare; in funzione di ciò, lo standard si compone di ventisei elementi descrittivi distribuiti in sette aree di descrizione, ovvero l'area dell'identificazione, delle informazioni sul contesto, delle informazioni relative al contenuto e alla struttura, delle informazioni relative alle condizioni di accesso e

[67] Gli standard sono disponibili, rispettivamente, ai link <https://www.iso.org/standard/73172.html> e <https://www.iso.org/standard/81600.html> (l'accesso è vincolato al pagamento delle risorse). Su ISO 23081 si vedano M. Guercio, *Conservare il digitale* cit., pp. 74.85; S. Pigliapoco, *Progetto archivio digitale* cit., pp. 76-83.

all'utilizzazione, delle informazioni relative alla documentazione collegata, delle note e del controllo della descrizione[68].

ISAAR(CPF), ovvero *International Standard Archival Authority Records for Corporate Bodies, Persons and Families*, è stato rilasciato nel 1996 per definire in maniera coerente e uniforme i soggetti produttori degli archivi. Sulla base di questa norma vengono realizzati dei *record di autorità* contenenti ventisette elementi descrittivi raccolti in quattro aree: l'area dell'identificazione (che include anche le forme normalizzate della denominazione dell'entità), l'area della descrizione, l'area delle relazioni e l'area di controllo[69].

ISDIAH, *International Standard for Describing Institutions with Archival Holdings*, risale al 2008 e ha l'obiettivo di fornire un quadro per la descrizione degli istituti che conservano collezioni archivistiche. Al fine di collegare le rappresentazioni espresse con gli schemi ISAD e ISAAR, si dispone in trentuno elementi descrittivi, distribuiti in area dell'identificazione, delle informazioni relative ai contatti, delle informazioni relative all'accesso e di controllo[70].

ISDF, *International Standard for Describing Functions*, è stato pubblicato nel 2007 e ha lo scopo di fornire un modello per la descrizione delle funzioni dei soggetti che producono e conservano archivi: questa particolare chiave di rappresentazione è utile a inquadrare la finalità dei documenti prodotti nel corso dello svolgimento di un determinato procedimento, al di là del soggetto produttore incaricato in un dato momento dello svolgimento della funzione interessata, ad individuare ulteriori chiavi d'accesso e a porre in evidenza le relazioni tra queste responsabilità, gli enti cui sono demandate e le risorse prodotte per il loro espletamento. Si articola in ventisei elementi, articolati, come per gli altri standard, in area dell'identificazione, delle informazioni sul contesto, delle relazioni e di controllo: le

[68] La seconda è più recente versione dello standard è consultabile, in traduzione italiana, al link <https://www.icar.beniculturali.it/fileadmin/risorse/docu_standard/RAS_2003_1.pdf>.

[69] La seconda è più recente versione dello standard è consultabile, in traduzione italiana, al link <https://www.icar.beniculturali.it/fileadmin/risorse/docu_standard/RAS_2003_1.pdf>.

[70] Lo standard è consultabile, in traduzione italiana, al link <https://www.icar.beniculturali.it/fileadmin/risorse/docu_standard/RAS_2007_2.pdf>.

informazioni da valorizzare obbligatoriamente sono la tipologia della funzione, la forma autorizzata del nome e il codice identificativo della descrizione della funzione[71].

Questi standard trovano la loro integrazione per l'applicazione digitale in EAD (*Encoded Archival Description*[72]) e EAC-CPF (*Encoded Archival Context for Corporate bodies, Persons and Families*[73]): l'equazione che rappresenta il rapporto tra questi standard vede ISAD in relazione a EAD come ISAAR a EAC. Entrambi *Document Type Definition* in linguaggio XML, mirano rispettivamente alle elaborazioni informatiche delle descrizioni effettuate sui modelli ISAD e ISAAR, perché sia possibile ricercarle, recuperarle, visualizzarle e condividerle[74].

RiC-CM (*Records in Contexts - A Conceptual Model for Archival Description*), infine, è uno standard descrittivo, corredato di una propria ontologia RiC-O (*Record in context – Onthology*), elaborato nell'ambito dell'ICA dal 2012 al 2016, di recente rilasciato alla pubblica consultazione. RiC si compone di quattro parti, che consistono rispettivamente in un'introduzione alla descrizione archivistica, nel modello concettuale vero e proprio, nella già citata ontologia (espressa formalmente in OWL[75]) e in linee guida per l'applicazione, non ancora ultimate.

RiC-CM è uno schema di alto livello che si focalizza sull'identificazione e la descrizione dei documenti, delle persone che li hanno creati e utilizzati e delle attività che interessano la produzione di tali *records*. RiC raccoglie gli input degli standard ISAD, ISAAR, ISDF, ISDF con l'obiettivo, però, di rappresentare

---

[71] Lo standard è consultabile in inglese al link <https://www.ica.org/sites/default/files/CBPS_2007_Guidelines_ISDF_First-edition_EN.pdf>. Si veda, in proposito, M. Guercio, *Archivistica informatica. I documenti in ambiente digitale*, Roma, Carocci Editore, 2015, pp. 253-255.

[72] Lo standard è consultabile alla pagina dedicata del sito web della Library of Congress al link <https://www.loc.gov/ead/>. Il *Technical Subcommittee on Encoded Archival Standards* (TS-EAS) ha finalizzato due modifiche minori di EAD3 (Tag Library) ed EAD 2002 (Schema), che lo *Standards Committee* ha approvato prima della pausa estiva. Questi cambiamenti avviano una fase di revisione maggiore, per cui il TS-EAS sta attualmente riferendosi alla *user community* per riceverne osservazioni e *feedback*.

[73] Lo standard è consultabile nel sito web apposito, curato dalla *Staatsbibliothek zu Berlin*, al link <https://eac.staatsbibliothek-berlin.de/>.

[74] Sugli standard ISAD(G), ISAAR (CPF), ISDIAH, EAD ed EAC si vedano P. Carucci, M. Guercio, *Manuale di archivistica*, Roma, Carocci Editore, 2013, pp. 137-163; M. Grossi, *Gli standard per la descrizione archivistica,* in *Archivistica informatica. I documenti in ambiente digitale*, Roma, Carocci Editore, 2015, pp. 233-275; S. Pigliapoco, *Progetto archivio digitale* cit., pp. 22-24;

[75] *Web Ontology Language*, standard del World Wide Web Consortium (<https://www.w3.org/OWL/>).

le entità in quanto tali, come base per la descrizione senza anticiparne il prodotto finale: interessa le istanze fisiche dei record, ma non copre tutti gli attributi e le relazioni che necessari per gestirle materialmente. Per accogliere ulteriori descrizioni relative alla dimensione analogica, RiC-CM è pensato per essere estensibile, sia attraverso il processo formale di sviluppo e manutenzione degli standard ICA, sia attraverso l'uso di standard esistenti che riguardano gli attributi e le relazioni necessarie per la conservazione dei documenti cartacei[76].

[76] Lo standard è consultabile in inglese al link <https://www.ica.org/sites/default/files/ric-cm-02_july2021_0.pdf>.

Parte II. La conservazione digitale in Italia

II.1 La conservazione della memoria digitale

Il tema della conservazione della memoria, in Italia, riveste grande importanza sin dall'epoca medievale: il nodo fondamentale delle modalità di tenuta degli archivi è la pubblica fede dei documenti conservati. Da qui, il percorso avviato dall'attività dell''archivista non teorico' Ludovico Antonio Muratori nel XVIII secolo, attraverso le riflessioni e i dibattiti ottocenteschi, è giunto, nel Novecento, alla sua maturazione: non solo si è arrivati all'affermazione del dominio dei beni culturali sugli archivi, ma anche alle definizioni concettuali e alle necessità operative delle fasi corrente, di deposito e storico degli archivi[1]. Espressioni di tale complessità di pensiero si trovano nella Legge archivistica del 1963[2] e le disposizioni del Codice dei Beni Culturali[3] in materia di archivi: l'autorità archivistica interviene sin dalle fasi di selezione e scarto ed possiede estese competenze sulla conservazione perenne dei documenti, in un'ottica che tiene in considerazione l'oggetto archivistico tanto nelle sue caratteristiche giuridico-amministrative, tanto del suo valore come parte del patrimonio culturale.

Questa profonda e secolare cultura archivistica ha consentito, nel momento chiave di inizio della riflessione sull'introduzione del digitale, di poter impostare discussioni concettuali e metodologiche di rilievo e aperte al panorama internazionale, a partire dalle considerazioni sugli obiettivi della disciplina archivistica trasposti sul digitale e sul cambiamento delle dinamiche di conservazione della memoria dall'analogico al digitale: il preservare le risorse digitali implica, infatti, ancora maggior cura nella conservazione delle informazioni sui contesti dei documenti stessi, per poterne non solo ricostruire lo scopo e le vicende, ma per poterli effettivamente rendere leggibili e utilizzabili. È importante che venga lasciata traccia non solo delle modalità di produzione, ma anche dei processi di migrazione

[1] Si veda, per gli spunti diacronici citati sulla tradizione archivistica italiana (posti in questa forma di accenno ai soli fini introduttivi) E. Lodolini, *Storia dell'archivistica italiana. Dal mondo antico alla metà del secolo XX,* Milano, Franco Angeli, 2013.

[2] Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 *Norme relative all'ordinamento ed al personale degli archivi di Stato*.

[3] Decreto Legislativo 22 gennaio 2004 n. 42 *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*.

e versamento, affinché si abbia garanzia dell'affidabilità e dell'autenticità dell'oggetto. La fase di passaggio in custodia è cruciale: vi è un passaggio di responsabilità che prevede il versamento in un sistema che debba possedere requisiti che interessano le componenti tecnologiche e di sicurezza, i processi e le funzionalità, l'organizzazione, le competenze e i ruoli, per poter garantire a lungo termine l'integrità e l'autenticità e, in particolare, assicurare l'accesso alle risorse, custodite in un ambiente differente rispetto a quello della loro formazione e gestione[4]. È necessario, per questi aspetti, procedere con un approccio dinamico e di continuo aggiornamento, in considerazione delle evoluzioni del contesto digitale e normativo, che tenga conto dell'esigenza di documentare le scelte intraprese e le motivazioni relative all'adozione di determinati strumenti e *policies* o al loro cambiamento.

Questi spunti hanno spinto anche ad analizzare come, nel digitale, si debbano collocare le tre età dell'archivio: la conservazione, in ambito analogico, è prerogativa della fase storica, mentre con il passaggio al digitale coinvolge non solo quella di deposito, ma, per gli aspetti di pianificazione, anche la fase corrente. L'aspetto che in normativa e per prassi risalta maggiormente è la chiave di lettura del sistema di conservazione digitale come archivio di deposito: pur essendo previsto che possa avvenire anche all'interno dei sistemi di gestione e anticipatamente rispetto al versamento in conservazione, si tende comunque a considerare lo scarto come operazione da compiersi all'interno di quest'ultimo sistema, lasciando, in ogni caso, la documentazione residua alla selezione all'interno dello stesso. A tal proposito, è ancora in corso di definizione, sia in normativa sia nell'ambito delle effettive realizzazioni, il percorso per 'perennizzare' il patrimonio culturale archivistico digitale: sebbene vi sia un insieme di norme piuttosto corposo, vi è ancora non sufficiente linearità su questi aspetti[5].

Le riflessioni si diramano anche nell'analisi della transizione al digitale sull'archiveconomia: la consistenza fisica degli archivi e dei documenti digitali, infatti, cambia radicalmente e perde la prevalenza tipica dell'analogico. Questo passaggio dall''unità di misura' dal metro lineare ai *bytes* implica l'adozione di criteri completamente diversi nella

[4] M. Guercio, *Conservare il digitale* cit., pp. 23-34.

[5] F. Delneri, *Il documento amministrativo informatico: un cammino per approssimazione. Criticità e risposte possibili, tra normativa e prassi, dalla formazione alla conservazione* «JLIS.it Italian Journal of Library, Archives and Information Science» 8 (2017), 3, pp. 26-38, disponibile online al sito <https://www.jlis.it/article/view/12193/11275>.

valutazione delle dimensioni degli archivi e della capacità di memorizzazione dei sistemi di storage[6].

Queste discussioni hanno avuto significativa spinta nel periodo tra 2010 e 2014, anni in cui si è costituita abbondante bibliografia sul tema e si è sviluppata gran parte della normativa di settore, per poi svilupparsi sino al momento attuale, in cui risulta attiva in particolare nei contesti pubblico-istituzionali dell'Agenzia per l'Italia Digitale[7], della Direzione Generale degli Archivi[8], dell'iniziativa Forum PA[9], e nel mondo accademico e della ricerca attraverso corsi e progetti organizzati da molti Atenei[10] e dall'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD)[11].

Ciò nonostante, si è nel tempo radicata una dicotomia che, ancora oggi, costituisce un limite per l'elaborazione di norme e strategie omogenee non solo sulla conservazione a lungo termine di documenti e archivi digitali, ma anche sulla loro gestione: come è già stato evidenziato in contesto europeo, vi è un distaccamento i tentativi del legislatore di perimetrare questi ambiti dal punto di vista amministrativo e le riflessioni dell'ambito storico culturale[12]. Questo si risolve nella più onerosa conseguenza dell'esclusione del Ministero della Cultura e delle sue ramificazioni dall'operatività e dall'elaborazione di provvedimenti in relazione a questi aspetti: di fatto, quest'ultimo non viene interpellato direttamente per la stesura dei dispositivi, ma gli sono conferite soltanto le funzioni di controllo sulla selezione e sullo scarto della documentazione delle pubbliche amministrazioni o di interesse storico[13].

A tal proposito, si rileva inoltre come gli aspetti connessi alla tutela degli archivi digitali, siano ancora in fase di definizione: sebbene con il DPCM 2 dicembre 2019 n. 169, ovvero il

---

[6] S. Allegrezza, *Verso una nuova archiveconomia: alcune riflessioni sull'evoluzione della disciplina nella transizione dall'analogico al digitale*, «JLIS.it Italian Journal of Library, Archives and Information Science», 8 (2017), 1, pp. 114-126, disponibile online al sito <https://www.jlis.it/article/view/12140/11226>.

[7] Da qui in avanti AgID. Si veda, in proposito, il sito web <https://www.agid.gov.it/>.

[8] Si veda, in proposito, il sito web <http://www.archivi.beniculturali.it/>.

[9] Si veda, in proposito, il sito web <https://www.forumpa.it/>.

[10] Si citano, a titolo esemplificativo, le Università con corsi di studio e progetti di ricerca avviati sul tema, ovvero la Sapienza, l'Alma Mater Studiorum (Campus di Ravenna), l'Università della Calabria, l'Università di Macerata e l'Università di Pisa.

[11] <http://www.aiucd.it/>.

[12] S. Pigliapoco, *Digital Preservation in Italy: Reflections on Models, Criteria and Solutions*, «JLIS: Italian Journal of Library, Archives and Information Science», 10 (2019), 1, pp. 1-11, <https://www.jlis.it/article/view/12521/11349>.

[13] Questa circostanza si noterà evidentemente nel capitolo II.2, a cui si rimanda per le specifiche citazioni della normativa.

regolamento di organizzazione del Ministero per i beni e le attività culturali e per il turismo, si sia tentato di recuperare le funzioni di tutela anche sugli archivi digitali, di fatto questo è rimasto un riconoscimento formale, viste anche le difficoltà insite all'esercizio di tale facoltà su documenti privi degli elementi fisici[14].

Un punto di incontro sembra essere costituito, però, dai Poli di conservazione[15]: istituiti nell'ambito di enti territoriali o organismi che appartengono agli apparati operativi statali, possiedono anche la qualifica di conservatori accreditati, fattori che li rendono tanto sensibili alle istanze e agli obblighi riguardanti la pubblica amministrazione e il settore dei beni culturali tanto alle dinamiche proprie di soggetti terzi fornitori di servizi di conservazione.

[14] Si vedano, in proposito, i contributi A.Alfier, *La tutela degli archivi digitali: prime esplorazioni dell'hic sunt leones?*, «Archivi», XVI, 2 (2021), Padova, Cleup, 2021, pp. 6-18; A. Pieri, D. Robotti, *La tutela degli archivi digitali degli enti pubblici: un sistema ancora da progettare*, «Archivi», XIV, 2 (2019), pp. 197-203; P. Santoboni, *Il percorso per la definizione di un modello di prassi archivistica per la vigilanza sugli archivi digitali*, «Archivi», XVI, 2 (2021), Padova, Cleup, 2021, pp.

[15] Si veda, a tal proposito, il capitolo II.3.

II.2 La normativa in materia di conservazione digitale: iter e svolte recenti

Il quadro sopra illustrato si compone anche dei tentativi, a partire dai primi anni duemila, di disciplinare l'ambito della conservazione digitale, al fine tanto di tutelare il valore giuridico dei documenti digitali e la loro usabilità nell'ambito della fase di deposito, quanto di salvaguardare la loro sopravvivenza come memoria storica.

In questo paragrafo si ripercorre l'iter normativo intrapreso dalla versione originaria del CAD alle sue modifiche seguenti al Decreto Legge 16 luglio 2020 n. 76 *Misure urgenti per la semplificazione e l'innovazione digitale*[1] e dalle *Regole tecniche in materia di sistemi di conservazione* alle *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico* al fine di comprendere, in prospettiva diacronica, le scelte del legislatore italiano per giungere all'attuale contesto.

Il Codice dell'Amministrazione Digitale

Il riferimento normativo con cui avviare questa ricostruzione è costituito dal Decreto Legislativo n. 82 del 2005, il Codice dell'Amministrazione Digitale[2]: in questo dispositivo si trovano i riferimenti primari per la conservazione dei documenti informatici, da cui discendono le successive regolamentazioni tecniche e linee guida. Riguardo alla sua versione originaria risalente al 2005[3], sono da evidenziare due circostanze. Innanzitutto, la conservazione dei documenti informatici è intesa come conservazione sostitutiva: vi era stabilito che i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, riprodotti su supporti informatici, fossero validi e rilevanti a tutti gli effetti di legge se la riproduzione venisse effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche previste dallo stesso CAD[4]; i

[1] Da qui in avanti Decreto Semplificazioni.

[2] Decreto legislativo 7 marzo 2005 n. 82 *Codice dell'Amministrazione Digitale* (da qui in avanti CAD).

[3] Si veda, per una breve sintesi 'storica' sul CAD, G. Manca, *Breve storia della PA digitale: la genesi e l'evoluzione del Codice dell'Amministrazione Digitale*, «Agenda Digitale», 6 luglio 2020, disponibile online al sito <https://www.agendadigitale.eu/cittadinanza-digitale/breve-storia-della-pa-digitale-la-genesi-e-levoluzione-del-codice-dellamministrazione-digitale/>.

[4] Art. 43 CAD Riproduzione e conservazione dei documenti «1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro

requisiti fissati per la conservazione dei documenti informatici prevedevano che il sistema di conservazione dei documenti informatici garantisse l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento, l'integrità del documento, la leggibilità e la reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari e il rispetto delle misure di sicurezza previste dal Decreto Legislativo del 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali*[5].

Il secondo punto da porre in rilievo riguarda la definizione delle Regole tecniche: nella prima versione del CAD la modalità prevista per emanare questo provvedimento è costituita da decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, in coordinazione con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate nel presente codice, sentita la Conferenza unificata ed il Garante per la protezione dei dati personali nelle materie di competenza[6].

conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71. 2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali. 3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali. 4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42» (versione previgente al D.Lgs. 30 dicembre 2010, n. 235).

[5] Art. 44 CAD Requisiti per la conservazione dei documenti informatici «1. Il sistema di conservazione dei documenti informatici garantisce: a. l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; b. l'integrità del documento; c. la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i' dati di registrazione e di classificazione originari; d. il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto». (versione previgente al D.Lgs. 30 dicembre 2010, n. 235).

[6] Art. 71 CAD Regole tecniche «1. Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate nel presente codice, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, ed il Garante per la protezione dei dati personali nelle materie di competenza, in modo da garantire la coerenza tecnica con le regole tecniche sul sistema pubblico di connettività di cui all'articolo 16 del decreto legislativo 28 febbraio 2005, n. 42, e con le regole di cui al disciplinare pubblicato in allegato B al decreto legislativo 30 giugno 2003, n. 196. 2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo» (versione previgente al D.Lgs. 30 dicembre 2010, n. 235).

Il CAD è stato poi modificato e integrato da numerosi dispositivi[7]: quelli rilevanti sul tema della conservazione digitale sono, in particolare, il D.Lgs. 30 dicembre 2010 n. 235[8], il D.Lgs. 26 agosto 2016 n. 179[9], il D.Lgs. 13 dicembre 2017 n. 217[10] e il già citato Decreto Semplificazioni.

La versione del CAD successiva alle modifiche determinate dal D.Lgs. 30 dicembre 2010, n. 235 presenta delle significative novità: si è introdotto lo status di conservatore accreditato, che ha rappresentato, sino all'avvento delle *Linee Guida* AgID, un concetto cardine del 'sistema conservazione digitale'. Questi vengono definiti come «soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza[11]».

Si estende, inoltre, ciò che riguarda i requisiti per la conservazione digitale: si stabilisce che il sistema di conservazione dei documenti informatici venga gestito da un responsabile, che opera d'intesa col responsabile del trattamento dei dati personali e con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli

[7] Oltre ai provvedimenti che di seguito si elencano, vi sono anche, tra gli altri, il D. Lgs. 4 aprile 2006, n. 159, D.L. 24 dicembre 2007, n. 244, D.L. 28 gennaio 2009 n. 2, D.L.18 giugno 2009, n. 69, D.L. 3 agosto 2009, n. 102, D.Lgs. 30 dicembre 2010, n. 235, D.L. n. 221/2012, D.L. n. 98/2013.

[8] Decreto Legislativo 30 dicembre 2010, n. 235 *Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69*.

[9] Decreto Legislativo 26 agosto 2016, n. 179 *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*.

[10] Decreto Legislativo 13 dicembre 2017, n. 217 *Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*.

[11] Art. 44-bis c. 1 CAD *Conservatori accreditati* «1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA. 2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31» (versione previgente al D.lgs 179/2016. Si precisa queste citazioni normative sono attinte specificatamente dalla versione emanata immediatamente dopo l'entrata in vigore del decreto legislativo di modifica oggetto del paragrafo corrente; il riferimento *ante quem* vuole esprimere la cronologia anteriore rispetto alle integrazioni menzionate nel seguito).

archivi; tale Responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione[12].

Si inserisce, inoltre, l'obbligatoria acquisizione del parere tecnico di DigitPA (antecedente denominazione di AgID), per l'emanazione delle regole tecniche previste dal Codice per le modalità di esecuzione delle disposizioni[13].

Con il D.Lgs. 26 agosto 2016, n. 179., sono state apportate modifiche sia all'ambito della conservazione, sia alla regolamentazione tecnica inerente a quest'ultima, in parte conseguenti all'entrata in vigore del regolamento eIDAS. Innanzitutto, i fornitori di servizi di conservazione vengono collocati tra i soggetti che, per prestare servizi qualificati, devono rivolgere domanda ad AgID e rispettare le condizioni previste dal Regolamento 910/2014, venendo di fatto posti in similitudine con i *Trust Service Provider* definiti nello stesso Regolamento[14].

Ampliati risultano anche i requisiti fissati per la conservazione dei documenti informatici, che vengono, in questa versione del CAD, espressi unitamente a quelli per la gestione: a quanto già precedentemente definito, si aggiungono la sicurezza e l'integrità del sistema insieme alle garanzie d'accesso alla documentazione custodita[15].

---

[12] Artt. 43 *Riproduzione e conservazione dei documenti,* 44 *Requisiti per la conservazione dei documenti informatici* CAD (versione previgente al D.lgs 179/2016).

[13] Art. 71 CAD *Regole tecniche* (versione previgente al D.lgs 179/2016).

[14] Art. 29 CAD *Qualificazione e accreditamento* «1. I soggetti che intendono avviare la prestazione di servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata, di gestore dell'identità digitale di cui all'articolo 64, di conservatore di documenti informatici di cui all'articolo 44-bis presentano all'AgID domanda, rispettivamente, di qualificazione o di accreditamento, allegando alla stessa una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità accreditato dall'organo designato ai sensi del Regolamento CE 765/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008 e dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99. 2. Il richiedente deve trovarsi nelle condizioni previste dall'articolo 24 del Regolamento eIDAS. 3. Fatto salvo quanto previsto dall'articolo 44-bis, comma 3, del presente decreto e dall'articolo 14, comma 3, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, il richiedente deve inoltre possedere i requisiti individuati con decreto del Presidente del Consiglio dei ministri da fissare in base ai seguenti criteri: a) per quanto riguarda il capitale sociale, graduazione entro il limite massimo di cinque milioni di euro, in proporzione al livello di servizio offerto; b) per quanto riguarda le garanzie assicurative, graduazione in modo da assicurarne l'adeguatezza in proporzione al livello diservizio offerto» (versione previgente al D.lgs 13 dicembre 2017, n. 217).

[15] Art. 44 CAD *Requisiti per la gestione e conservazione dei documenti informatici* 1. Il sistema di gestione informatica e conservazione dei documenti informatici della pubblica amministrazione assicura: a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445; b) la sicurezza e l'integrità del sistema e dei dati e documenti presenti; c) la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita; d) la raccolta di

Per quanto riguarda le Regole tecniche, viene posta la responsabilità della proposta del provvedimento in capo all'Agenzia per l'Italia Digitale, ponendo ulteriore rilievo sulla funzione di questo ente per lo sviluppo di tale normativa[16].

Il D.Lgs. 13 dicembre 2017, n. 217, correttivo e integrativo rispetto al precedente Decreto legislativo, introduce delle altrettanto significative novità: viene rimosso l'articolo 44-bis sui conservatori accreditati e viene inserito il vincolo di aderenza alle modalità fissate dalle Linee guida per la domanda di accreditamento[17]. A tal proposito, significativa è anche la modifica

---

informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati; e) l'agevole reperimento delle informazioni riguardanti i documenti registrati; f) l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle disposizioni in materia di tutela dei dati personali; g) lo scambio di informazioni, ai sensi di quanto previsto dall'articolo 12, comma 2, con sistemi di gestione documentale di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi; h) la corretta organizzazione dei documenti nell'ambito del sistema di classificazione adottato; i) l'accesso remoto, in condizioni di sicurezza, ai documenti e alle relative informazioni di registrazione tramite un identificativo univoco; j) il rispetto delle regole tecniche di cui all'articolo 71. 1-bis. Il sistema di gestione e conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti conclusi» (versione previgente al D.lgs 13 dicembre 2017, n. 217).

[16] Art. 71 CAD *Regole tecniche* «1. Con decreto del Ministro delegato per la semplificazione e la pubblica amministrazione, su proposta dell'AgID, di concerto con il Ministro della giustizia e con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e il Garante per la protezione dei dati personali nelle materie di competenza, sono adottate le regole tecniche per l'attuazione del presente Codice» (versione previgente al D.lgs 13 dicembre 2017, n. 217).

[17] Art. 29 CAD *Qualificazione e accreditamento*. «1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività i gestore di posta elettronica certificata o di gestore dell'identità digitale di cui all'articolo 64 presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida. I soggetti che intendono svolgere l'attività di conservatore di documenti informatici presentano all'AgID domanda di accreditamento, secondo le modalità fissate dalle Linee guida. 2. Il richiedente deve trovarsi nelle condizioni previste dall'articolo 24 del Regolamento eIDAS, deve avere natura giuridica di società di capitali e deve disporre dei requisiti di onorabilità, tecnologici e organizzativi, nonché delle garanzie assicurative e di eventuali certificazioni, adeguate rispetto al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. I predetti requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei ministri, sentita l'AgID. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche. [..] 4. La domanda di qualificazione o di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa. 5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa. 6. A seguito dell'accoglimento della domanda, il AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto dal AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione» (versione previgente al Decreto Semplificazioni).

all'articolo 71, relativo al provvedimento tecnico da emanare in attuazione agli articoli del CAD: vengono introdotte le Linee Guida, che AgID è incaricata di redigere d'intesa con le amministrazioni competenti e il Garante per la protezione dei dati personali e di adottare previa consultazione pubblica[18].

Inoltre, vengono nuovamente esposti separatamente i requisiti del sistema di gestione e del sistema di conservazione, sebbene nella rubrica comune *Requisiti per la gestione e conservazione dei documenti informatici*: viene stabilito che il sistema di conservazione debba assicurare che i documenti in esso conservati mantengano caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo quanto indicato nelle Linee guida di cui si è già fatta menzione[19].

Come si vedrà nel successivo paragrafo su queste *Linee Guida* AgID, l'introduzione di queste ultime e la loro consultazione in Commissione Europea hanno determinato profonde

[18] Art. 71 CAD *Regole tecniche* «1. L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice. Le Linee guida divengono efficaci dopo la loro pubblicazione nell'apposita area del sito Internet istituzionale dell'AgID e di essa ne è data notizia nella Gazzetta Ufficiale della Repubblica italiana. Le Linee guida sono aggiornate o modificate con la procedura di cui al primo periodo. [..] 1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea» (versione previgente al Decreto Semplificazioni).

[19] Art. 44 CAD *Requisiti per la gestione e conservazione dei documenti informatici* «1. Il sistema di gestione informatica dei documenti delle pubbliche amministrazioni, di cui all'articolo 52 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è organizzato e gestito, anche in modo da assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida. 1-bis. Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi. 1-ter. 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. 1-quater. Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis» (versione previgente al Decreto Semplificazioni).

modifiche che hanno impattato anche sul CAD, eliminando, di fatto, la denominazione di conservatore accreditato e sostituendo alle dinamiche di accreditamento la qualificazione[20].

Nello specifico, il Decreto Semplificazioni ha implicato la modifica degli articoli che hanno per oggetto la conservazione digitale: innanzitutto (come si è già accennato), viene definitivamente rimosso il concetto di conservatori accreditati, così come eliminata è ogni menzione all'accreditamento[21].

Vengono, inoltre, definiti nello stesso CAD i modelli organizzativi per la conservazione per le Pubbliche amministrazioni *in house*, in *outsourcing* e misto[22], con il vincolo che queste due ultime opzioni possano essere effettuate soltanto attraverso soggetti terzi che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* e nel *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* emanato da AgID[23].

[20] Tali tematiche verranno dettagliatamente esposte nel par. successivo *Le Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico*; in questa sede ci si concentra sulle specifiche modifiche al CAD.

[21] Nel testo dell'art. 29 CAD *Qualificazione dei fornitori di servizi*, che nelle versioni previgenti al Decreto Semplificazioni includeva in rubrica l'accreditamento, vengono citati in maniera generale «i soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata»; viene descritto nel seguito l'iter di qualificazione.

[22] Questi erano in precedenza citati soltanto nel DPCM 3 dicembre 2013 *Regole tecniche in materia di sistemi di conservazione.* Si veda, in proposito, il successivo sottoparagrafo Le *Regole tecniche in materia di sistemi di conservazione* e l'accreditamento secondo la Circolare AgID n. 65/2014.

[23] Art. 34 CAD*, Norme particolari per le pubbliche amministrazioni*, c.1-bis « 1-bis. 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». Si veda, a proposito delle Linee guida e del Regolamento, il sottoparagrafo Le *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico* e il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*.

I requisiti per la conservazione dei documenti informatici restano i medesimi[24], così come immutate restano le disposizioni sulle Linee Guida[25].

Le *Regole tecniche in materia di sistemi di conservazione* e l'accreditamento secondo la Circolare AgID n. 65/2014

A dare compimento a quanto indicato dall'articolo 71 delle versioni previgenti al D.lgs 217/2017, nel 2013 sono state emanate le *Regole Tecniche in materia di sistemi di conservazione digitale*[26]: efficaci sino al gennaio 2022, data a partire dalla quale verranno sostituite dalle *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico* [27], raccolgono le disposizioni su sistemi di conservazione, oggetti della conservazione, modelli organizzativi, ruoli e responsabilità, responsabile della conservazione, Manuale di conservazione, processi, sicurezza e modalità di esibizione; agli allegati sono affidate, invece, le definizioni, le indicazioni sui formati, gli standard e le specifiche tecniche generali, le specifiche tecniche del pacchetto di archiviazione e i metadati

[24] Art. 44 CAD *Requisiti per la gestione e conservazione dei documenti informatici* «1. Il sistema di gestione informatica dei documenti delle pubbliche amministrazioni, di cui all'articolo 52 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è organizzato e gestito, anche in modo da assicurare l'indicizzazione e la ricerca dei documenti e fascicoli informatici attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida. 1-bis. Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi. 1-ter. 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. 1-quater. Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis»

[25] Art. 71 CAD *Regole tecniche*.

[26] Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del* 2005, da ora in avanti DPCM 3 dicembre 2013 (C).

[27] Sulla proroga dell'entrata in vigore delle *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico* (da qui in avanti Linee Guida AgID), si veda il par. *Le Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico*.

relativi al documento informatico, al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

Ciò che, in linea generale, è necessario evidenziare è la scelta – già a partire dal 2013 – del modello OAIS per la realizzazione dei sistemi di conservazione e per i processi di gestione dei pacchetti informativi, nell'ottica di favorire la semplicità architetturale e l'interoperabilità[28]: secondo questa stessa logica e con la finalità di garantire uniformità nel trattamento degli oggetti sottoposti a conservazione, nell'allegato 2 si fornisce una lista delle caratteristiche e dei formati adeguati al mantenimento delle risorse a lungo termine[29], nell'allegato 5 si definiscono i set di metadati per documenti e aggregazioni[30] e nell'allegato 4 è descritta la struttura del pacchetto di archiviazione, basato sullo standard UNI SiNCRO[31].

In più, vi è descritta una struttura organizzativa ben definita, con distribuzione di ruoli e compiti[32], tra cui spicca il Responsabile della conservazione: ha il compito di definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, di gestire i processi e di garantirne la conformità alla normativa vigente, di occuparsi della generazione del rapporto di versamento e del pacchetto di distribuzione (che lo stesso sottoscrive), di monitorare la correttezza delle funzionalità del sistema, di verificare periodicamente l'integrità degli archivi e della loro leggibilità, adottando misure adeguate in caso di rilevata obsolescenza e provvedendo, se necessario, alla produzione di copie o duplicati, di stabilire le *policies* per la sicurezza fisica e logica del

[28] Artt. 4, 9,10 DPCM 3 dicembre 2013 (C).

[29] Allegato 2 *Formati*. Sono presenti in tale elenco i formati PDF e PDF/A, TIFF, JPG, Office Open XML, Open Document Format, XML e TXT.

[30] Allegato 5 *Metadati*. I metadati minimi previsti per il documento informatico in questo documento sono: identificativo, riferimento temporale, soggetto produttore, oggetto e destinatario (cui il DPCM 3 novembre 2014 *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni* aggiunge l'impronta calcolata con funzione HASH SHA-256); per il documento amministrativo informatico si rimanda alla normativa sul protocollo informatico e sono: codice identificativo dell'amministrazione, codice identificativo dell'area organizzativa omogenea, codice identificativo del registro cui i documenti fanno riferimento, data di protocollo, numero di protocollo, oggetto, dati identificativi di mittente o destinatario, data e numero di protocollo se documento ricevuto, impronta del documento, indicazione della figura cui è in carico la gestione del documento, indice di classificazione, identificazione degli allegati e informazioni sul procedimento; i metadati minimi del fascicolo o aggregazione (per cui il riferimento è, di nuovo, il DPCM , infine, sono: identificativo, amministrazione titolare, amministrazioni partecipanti, responsabile del procedimento, oggetto, date di apertura e chiusura, codici identificativi documenti afferenti al fascicolo o all'aggregazione.

[31] Allegato 4 *Specifiche tecniche del pacchetto di archiviazione*. Su UNI SiNCRO si veda il capitolo II.3.

[32] Art. 6 DPCM 3 dicembre 2013 (C).

sistema, di assicurare la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite e di fornire agli organismi competenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza e di provvedere, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti[33]. Attiene a questa figura, infine, anche il dovere di predisporre il Manuale di conservazione: questo documento contiene informazioni sui soggetti che nel tempo hanno assunto la responsabilità del sistema, sull'intero funzionamento della struttura organizzativa, sulle tipologie degli oggetti conservati, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare a ciascuna, sulle modalità di presa in carico dei pacchetti di versamento, sul processo di conservazione e del trattamento dei pacchetti di archiviazione, sulle modalità di esibizione e di esportazione dal sistema con la produzione del pacchetto di distribuzione, sulle componenti tecnologiche, fisiche e logiche del sistema, con procedure di gestione e di evoluzione delle medesime, sulle procedure di monitoraggio e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie, sulla produzione di duplicati e copie, sui tempi di scarto, sulle modalità e le motivazioni per cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento e sulla normativa in vigore nei luoghi in cui sono conservati i documenti[34].

Altrettanto significativa è la definizione di tre modelli di conservazione: il primo consente lo sviluppo del sistema di conservazione presso l'organizzazione che deve custodire la propria documentazione; il secondo prevede l'affidamento totale del servizio a soggetti terzi, pubblici o privati, che erogano tali soluzioni in qualità di conservatori accreditati e il terzo contempla un'opzione mista di componenti *in house* e in *outsourcing*[35]. In proposito, il DPCM fa riferimento alla procedura di accreditamento dei conservatori: in particolare, si conferisce ad AgID il compito di definirne le modalità di espletamento e le prassi di

[33] Art. 7 DPCM 3 dicembre 2013 (C).
[34] Art. 8 DPCM 3 dicembre 2013 (C).
[35] Art. 5 DPCM 3 dicembre 2013 (C).

vigilanza[36]. Si è emanata dunque la Circolare n. 65 del 10 aprile 2014[37], che contiene le indicazioni sull'iter da seguire per ottenere tale qualifica: il sistema – ancora in vigore fino al primo gennaio 2022 – prevede la presentazione ad AgID, da parte del soggetto giuridico interessato, della domanda di accreditamento, con una serie di allegati che forniscono informazioni relative al richiedente, di tipo amministrativo, tecnico e organizzativo[38]. A seguito, AgID avvia l'attività istruttoria, basata su una *checklist* formulata in *compliance* con gli standard OAIS ed ETSI 101-533 ed effettuata da AgID stessa tramite organismo preposto o soggetti terzi, nel corso della quale il potenziale conservatore deve dare prova di conformità a determinati requisiti di qualità e sicurezza[39]. In caso di esito positivo dell'audit, la domanda di accreditamento viene accolta, il conservatore inserito nell'elenco ufficiale curato da AgID sul proprio sito istituzionale[40] ed è sottoposto ad attività di vigilanza da parte di quest'ultima[41].

Tra i requisiti richiesti figurano, in particolare, la prova della solidità economica e della capacità assicurativa del richiedente, la certificazione ISO 27001[42] per la sicurezza, la conformità a ISO 14721 e alle raccomandazione ETSI TS 101 533-1 V1.1.1[43] per

[36] Art. 13 DPCM 3 dicembre 2013 (C) «L'Agenzia per l'Italia digitale definisce, con propri provvedimenti, le modalità per l'accreditamento e la vigilanza sui soggetti di cui all'art. 44 -bis del Codice i quali adottano le presenti regole tecniche di cui al presente decreto per la gestione e la documentazione del sistema di conservazione, nonché per l'espletamento del processo di conservazione».

[37] Circolare n. 65 del 10 aprile 2014 Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

[38] L'elenco dei riscontri che il richiedente deve fornire ad AgID è contenuto nel documento integrativo alla Circolare 65/2014 'Accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici – documentazione per l'accreditamento', consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/documentazione/documentazione_per_accreditamento_conservatori_0.pdf>.

[39] Questi requisiti sono elencati nel documento integrativo alla Circolare 65/2014 'Accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici – Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza', consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/documentazione/requisiti_di_qualita_e_sicurezza_v.1.1.pdf>.

[40] La lista dei conservatori accreditati, contenente anche i rispettivi Manuali di conservazione, è consultabile al link <https://www.agid.gov.it/it/piattaforme/conservazione/conservatori-accreditati>. I numero totale attuale di soggetti accreditati come conservatori è 88.

[41] I criteri con cui viene condotta la vigilanza sono esplicitati nel documento Lista di riscontro per la visita ispettiva AgID e la certificazione di conformità – Descrizione della Lista di Riscontro per la visita ispettiva AgID e la certificazione di conformità dei conservatori accreditati, consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lista_di_riscontro_per_le_attivita_di_vigilanza_e_certificazione_di_conformita_v.1.pdf>.

[42] Si veda, in proposito, il capitolo II.3.

[43] Si veda, in proposito, il capitolo I.3.

l'implementazione del sistema di conservazione e della struttura organizzativa a supporto e a UNI SInCRO[44] per la struttura descrittiva dell'indice del pacchetto di archiviazione.

Viene, inoltre, estesa la rosa delle figure che intervengono sui processi di conservazione: al Responsabile della conservazione, vengono affiancate le figure di Responsabile del servizio di conservazione, Responsabile della funzione archivistica di conservazione, Responsabile del trattamento dei dati personali, Responsabile della sicurezza dei sistemi per la conservazione, Responsabile dei sistemi informativi per la conservazione e Responsabile dello sviluppo e della manutenzione del sistema di conservazione[45].

Da menzionare, infine, il tentativo nel 2015 di AgID di fornire indicazioni complessive in merito al tema con l'emissione del documento di indirizzo *Linee sulla conservazione dei documenti informatici*[46]: questo, prodotto anche in vista dei cambiamenti apportati da eIDAS e dalle modifiche al CAD e destinato sia alle Pubbliche amministrazioni sia ai privati, raccoglie informazioni e indicazioni sul documento e sul fascicolo informatico elaborate anche sulla base delle norme estratte dal CAD, sugli organismi di tutela e vigilanza, sui requisiti per i sistemi di conservazione dal DPCM 3 dicembre 2013 (C), sulle procedure di accreditamento per conservatori e sulle attività che il soggetto produttore deve compiere per predisporre e gestire correttamente i processi di conservazione tarate sulla scelta del modello organizzativo.

Le *Linee Guida sulla formazione, gestione e conservazione del documento informatico* e il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*

La pubblicazione sul sito istituzionale AgID, il 9 settembre 2020, delle *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico*[47] ha sancito una svolta

[44] Si veda la nota 31.

[45] Sulle figure professionali che è necessario inserire in organico, si veda il documento 'Accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici profili professionali', consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/documentazione/profili_professionali_per_la_conservazione.pdf>.

[46] Il documento è consultabile online al link <https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/la_conservazione_dei_documenti_informatici.pdf>.

[47] Le Linee Guida sono consultabili nella sezione Trasparenza del sito istituzionale AgID al link <https://trasparenza.agid.gov.it/archivio19_regolamenti_0_5385.html>; il Comunicato relativo alla loro

significativa per l'ambito conservazione digitale, in particolare a seguito del vaglio di questo provvedimento in Commissione Europea.

Per contestualizzare, le Linee Guida raccolgono in un dispositivo unitario i precedenti DPCM relativi agli stessi argomenti[48], articolandosi nelle sezioni Formazione dei documenti informatici, Gestione documentale e Conservazione[49]; a corredo del documento si trovano gli allegati, cui sono stati riservati gli aspetti maggiormente sensibili a modifiche e integrazioni[50].

L'attuale parte relativa alla conservazione evidenzia, rispetto alle disposizioni precedenti di cui si è parlato nel paragrafo precedente e alla versione in bozza, diversi aspetti particolarmente impattanti. Per rintracciare le cause di tali modifiche, è necessario risalire al già citato passaggio delle Linee Guida in Commissione Europea[51]. La prima bozza è stata rilasciata per la consultazione nel maggio 2019, per essere poi sottoposta alla Commissione, in versione semi-definitiva, l'anno successivo. Si è così adempiuto all'obbligo, indicato dal Regolamento europeo 1507/2015[52], di sottoporre i progetti di regole tecniche alla

adozione è stato pubblicato nella Gazzetta Ufficiale n. 259 del 19 ottobre 2020. Come da art. 71 del CAD, le Linee Guida sono entrate in vigore dal giorno della loro pubblicazione sul sito istituzionale di AgID, mentre la loro efficacia era prevista, inizialmente, a partire dal duecento settantesimo giorno da quest'ultima. Il provvedimento, nel seguito dell'elaborato, verrà citato anche come 'Linee Guida' e 'Linee Guida AgID'.

[48] Ci si riferisce, nello specifico, al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*; Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*; Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*.

[49] Per l'articolazione dettagliata dei capitoli, si rimanda al testo del provvedimento stesso, per cui si veda la nota 47.

[50] Gli allegati sono, rispettivamente: *Allegato 1 Glossario dei termini e degli acronimi*, *Allegato 2 Formati e file di riversamento*, *Allegato 3 Certificazione di processo*, *Allegato 4 Standard e Specifiche tecniche*, *Allegato 5 I metadati*, *Allegato 6 Comunicazione tra AOO di Documenti Amministrativi Protocollati*.

[51] Per le notizie relative al passaggio in commissione, il riferimento è costituito dagli aggiornamenti esposti da Patrizia Gentile, responsabile del Servizio Documentali e area trasformazione digitale, nonché coordinatrice gruppo definizione Linee Guida presso AgID, nel corso del *seminario Dibattito sulle nuove Linee Guida AgiD* tenutosi il 22 ottobre 2020 e organizzato dall'Associazione Nazionale Operatori e Responsabili della Custodia di contenuti digitali (da ora in avanti ANORC).

[52] Si veda il capitolo I.3.

Commissione, la quale può emettere pareri circostanziati che producono modifiche mandatorie al documento presentato.

All'invio del documento sono seguite interlocuzioni informali per chiarire il senso del testo, in particolare sul punto della localizzazione dei dati su territorio nazionale e sul procedimento di accreditamento dei conservatori, che hanno comunque risolto la consultazione in un parere circostanziato: nonostante i tentativi da parte di AgID di mantenere l'accreditamento, rinunciando a priori al discorso sulla localizzazione dei dati, è stato sostenuto che i regolamenti e le direttive europee già prevedono che tutti i servizi informatici in generale debbano rispettare le caratteristiche di qualità e sicurezza che, per l'accreditamento, si richiedono ai conservatori[53]; è stato menzionato, inoltre, il regolamento UE 1807/2018[54] sulla libera circolazione dei dati, in base al quale è stato rappresentato che il processo accreditamento costituisca infrastruttura inutile e dannosa per la libera circolazione dei dati.

La prima conseguenza di tale processo è consistita nella rimozione del requisito della localizzazione dei dati su territorio nazionale. Riguardo al tema dell'accreditamento, si è dovuto provvedere alla rettifica della normativa primaria che lo prevedeva: come si è visto, con l'art. 25 del Decreto Semplificazione, è stata disposta la modifica del CAD nei punti in cui si fa riferimento a questa procedura. Conseguentemente, sono stati rimossi i riferimenti all'accreditamento nelle Linee Guida e vi sono stati esplicitamente inseriti come requisiti gli standard internazionali ISO/IEC e ISO 14721 e le raccomandazioni ETSI TS 101 533-1 v. 1.2.1, che, appositamente, i conservatori accreditati già possiedono[55].

Questo ha comportato anche il dover sostituire l'apparato documentale e le procedure inerenti all'accreditamento: in sostituzione alla Circolare 65/2014 e ai documenti correlati, AgID ha emesso il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*[56], che contiene i requisiti generali e i requisiti di qualità, di sicurezza

[53] *Ibidem.*
[54] *Ibidem.*
[55] Questa circostanza è stata resa nota alla Commissione Europea, facendo presente che questi standard siano internazionali e previsti anche in ambito europeo, ma è stato ribadito che comunque l'accreditamento pone troppi vincoli per il fatto anche di dover porre la domanda a un ulteriore ente regolatore).
[56] Adottato con Determinazione n. 455/2021, il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* è consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/regolamento_sui_criteri_di_conservazione.pdf>.

e organizzazione necessari[57] e introduce il marketplace per i servizi di conservazione come sezione autonoma del Cloud Marketplace per le Pubbliche amministrazioni[58]. In questo regolamento sono fissate le indicazioni sia per i soggetti pubblici sia privati che erogano soluzioni di conservazione per conto delle PA: è esplicitato, tuttavia, che l'iscrizione al Marketplace non è obbligatoria, ma che i conservatori che intendono partecipare a procedure di affidamento pubbliche debbano ugualmente possedere i requisiti previsti nel regolamento ed essere sottoposti all'attività di vigilanza di AgID[59]. È importante evidenziare che viene appositamente esclusa la comprensione, tra le casistiche disciplinate dal provvedimento, dei servizi di conservazione a lungo termine disciplinati dal Codice dei Beni Culturali, con le conseguenti attività di vigilanza e sanzionamento[60]. La nuova procedura prevede la trasmissione di apposita richiesta secondo le modalità previste dalle Circolari AgID n. 2 e n. 3 del 9 aprile 2018 per l'iscrizione al Cloud Marketplace[61]. Dunque, acquisita la richiesta, AgID provvede entro trenta giorni alla verifica formale della documentazione prevista: in caso di documentazione erronea o incompleta AgID comunica al conservatore interessato i motivi che impediscono l'accoglimento dell'iscrizione, mentre in caso di documentazione idonea il conservatore viene inserito nel Marketplace. In ogni caso, è riservato all'Agenzia il diritto di verificare in ogni momento il possesso dei requisiti previsti, secondo le modalità stabilite dal regolamento recante le modalità per la vigilanza[62].

I requisiti per l'erogazione del servizio sono elencati in apposito allegato al Regolamento e sono suddivisi in generali (RG), di qualità (RQ) e di sicurezza (RS)[63]. Tra le novità da

[57] Per l'elencazione dei requisiti è stata scelta la forma dell'allegato.

[58] Le disposizioni relative al Cloud Marketplace sono contenute nella Circolare N. 2 del 9 aprile *2018 Criteri per la qualificazione dei Cloud Service Provider per la PA* (consultabile al link <https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/181151234430O__OCircolare+2-2018_Criteri+per+la+qualificazione+dei+Cloud+Service+Provider+per+la+PA.pdf>) e nella Circolare N. 3 del 9 aprile 2018 *Criteri per la qualificazione di servizi SaaS per il Cloud della PA* (consultabile al link <https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/181151237210O__OCircolare+3-2018_Criteri+per+la+qualificazione+di+servizi+SaaS+per+il+Cloud+della+PA+%28002%29.pdf>).

[59] Art. 3 *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*.

[60] Art. 1 *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*.

[61] Circolare n. 2 del 9 aprile 2018 *Criteri per la qualificazione dei Cloud Service Provider per la PA*; Circolare n. 3 del 9 aprile 2018 *Criteri per la qualificazione di servizi SaaS per il Cloud della PA*.

[62] Art. 4, commi 1-4 *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*; il riferimento alla vigilanza è il *Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. I) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni*.

[63] Allegato A *Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni*.

evidenziare rispetto alle disposizioni precedenti vi è l'inserimento delle raccomandazioni ETSI 319 401, riguardo cui è importante sottolineare che costituiscono i requisiti su cui si basa la valutazione dei Trust Service Provider per servizi qualificati eIDAS, in particolare in considerazione delle novità introdotte dalla proposta di modifica di quest'ultimo[64], di ISO 16363[65], ISO 37001 e ISO/IEC 22313, e l'inserimento di ISO 20000 come alternativa a ISO 9001[66]. In appendice all'allegato sono presenti le figure professionali previste: si approfondiscono, in tale sede, i compiti del Responsabile servizio di conservazione e del Responsabile della funzione archivistica di conservazione.

Tornando alle Linee Guida AgID, passando al dettaglio delle novità che introducono, si rileva che, in linea generale le funzioni, i processi, i modelli e i ruoli della conservazione digitale restano pressoché inalterati, ma vi sono delle modifiche terminologiche e operative[67].

Innanzitutto, vi sono delle variazioni sulle definizioni per i ruoli individuati nel processo di conservazione, ora definiti Titolare dell'oggetto della conservazione (che sostituisce la definizione di Soggetto Produttore), Produttore dei PdV (già Produttore) e Utente abilitato (già Utente), mentre restano invariati il Responsabile della Conservazione e il Conservatore; si introduce, però, la possibilità per i soggetti diversi dalla Pubblica Amministrazione di esternalizzare il ruolo del Responsabile della Conservazione, individuando in ogni caso un soggetto in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore.

Vengono esplicitamente citati all'interno del provvedimento stesso, diversamente dal DPCM 3 dicembre 2013 (C) per cui gli standard venivano collocati in un apposito allegato[68] e considerati opzionali, ISO/IEC 27001, OAIS e ETSI TS 101 533-1 v.1.2,. e viene riportata l'indicazione, per la struttura dell'indice di conservazione, dello standard UNI SiNCRO, elementi poi replicati nel Regolamento sulla fornitura dei servizi di conservazione.

---

[64] Si vedano, in proposito, i capitoli I.2 e I.3.

[65] Si veda, in proposito, il capitolo I.3.

[66] Si veda, su questi standard, il capitolo II.3.

[67] L'analisi delle Linee Guida AgID è stata effettuata nell'ambito delle attività svolte presso l'azienda Namirial S.p.A.: ne sono risultati i documenti interni *Nuove Linee Guida AgID 2020 sulla formazione, gestione e conservazione del documento informatico – Analisi e commento* e *Nuove Linee Guida AgID 2020 sulla formazione, gestione e conservazione del documento informatico – Documento operativo*, redatti con il Responsabile della funzione archivistica Enrico Giunta e la consulenza di supporto di Fabrizio Lupone.

[68] Allegato 5 al DPCM 3 dicembre 2013 (C) *Standard e specifiche tecniche*.

Relativamente agli aspetti procedurali, vi è nelle Linee guida una migliore definizione della fase di rifiuto del PdV, l'introduzione della possibilità di sottoscrivere l'indice del PdA anche con il sigillo elettronico qualificato o avanzato, intestato al Conservatore o al Titolare dell'oggetto da conservare, insieme alla firma digitale e qualificata: la sottoscrizione con firma elettronica può avvenire da parte o del Responsabile della conservazione o del Responsabile del servizio di Conservazione (unica soluzione precedentemente in essere). Tale novità sull'utilizzo del sigillo elettronico riguarda anche i pacchetti di distribuzione rilasciati su richiesta degli utenti.

Vi è, infine, l'obbligo, per il fornitore del servizio di conservazione, di mantenere e rendere disponibili le descrizioni del sistema all'interno del territorio nazionale e di garantire alle amministrazioni l'accesso elettronico effettivo e tempestivo ai dati conservati, indipendentemente dallo Stato membro nel quale si trovano questi dati.

Riguardo ai metadati, nell'allegato 5 si riuniscono i set minimi da applicare al documento informatico, al documento amministrativo informatico e alle aggregazioni documentali informatiche, precedentemente elencati in diversi provvedimenti. Nello specifico, i metadati minimi già indicati nei DPCM 3 dicembre 2013 e 13 novembre 2014 vengono per lo più confermati o riformulati, con l'aggiunta, tuttavia, di un numero cospicuo di nuovi campi obbligatori, talvolta articolati in sottocampi; è di notevole importanza l'inserimento degli schemi XSD di metadati, ai fini dell'adozione del nuovo UNI SiNCRO.

In linea di massima non risulta che i sistemi di conservazione, visto e valutato il contenuto delle Linee Guida, necessitino di modifiche di tipo sostanziale dal punto di vista strutturale e infrastrutturale.

Importanti, però, risultano i cambiamenti in relazione al rilascio della versione 2020 dello standard UNI SiNCRO, adottato all'interno del provvedimento e per il quale occorrerà predisporre nuove versioni dell'indice del PdA, la definizione del nuovo set di metadati minimi obbligatori piuttosto esteso rispetto al precedente e l'inserimento di diversi formati all'interno della lista degli ammessi per normativa.

Per quanto riguarda UNI SiNCRO e i metadati, da un lato vi sono i cambiamenti alle "macroaree" descritte, che si ripercuotono sulla struttura degli indici dei pacchetti

informativi, dall'altro vi è la gestione dei nuovi metadati minimi obbligatori di cui all'Allegato 5 delle *Linee Guida*: nello specifico, oltre al numero degli indici, si rende necessario stabilire come gestire la ripartizione in campi e sottocampi, ma anche l'utilizzo di valori prestabiliti alternati a campi liberi. La soluzione per integrare la struttura UNI SiNCRO con i nuovi metadati obbligatori si può rintracciare nell'utilizzo degli schemi XSD posti dell'allegato 5: alcuni dei metadati minimi obbligatori richiesti sono già valorizzati nell'indice del PdV e quindi associati al SiNCRO, ma, in caso di tali ridondanze, i metadati vanno inseriti comunque, procedendo se possibile a un'eventuale semplificazione.

Relativamente ai formati, è da evidenziare l'inserimento di tre tipologie particolarmente interessanti, vista la quantità particolarmente ristretta di possibilità esposte nel precedente Allegato 2 al DPCM 3 dicembre 2013 (C), ovvero dei maggiori formati di compressione[69] e di moltissimi formati audio e video[70], oltre a un elenco piuttosto esteso di formati di altro tipo[71]. In particolare, la valutazione di archivi compressi contenenti più oggetti informatici può essere considerata la base per l'implementazione della gestione delle aggregazioni documentali o dei fascicoli, a partire da quanto specificato nell'allegato sui metadati. Va però notato che il TXT non è più compreso nella lista dei formati ammessi per la conservazione.

Alla luce di quanto stabilito nelle nuove *Linee Guida*, è necessario inoltre considerare le variazioni che verranno apportate ai Manuali di Conservazione: in primo luogo, le variazioni terminologiche definite all'interno delle *Linee Guida* determinano la necessità di sostituzione di alcune denominazioni; in secondo luogo, l'entrata in vigore delle Linee Guida e il rilascio della versione 2020 di UNI SiNCRO, implicano la sostituzione di tutti i riferimenti alla normativa precedente e sostituita da questi nuovi provvedimenti: a questo proposito, sono da sottoporre a revisione tutte le sezioni che contengono riferimenti alla procedura di accreditamento, a seguito della sua rimozione, come stabilito dal *Decreto Semplificazione* e dalle revisioni alle *Linee Guida* della Commissione Europea.

[69] Si citano, ad esempio, i formati TAR, ZIP, GZIP, 7Z, ISO.
[70] Si citano, ad esempio, i formati DICM, MPEG 2, PART 2, MPEG 4, PART 14.
[71] Si citano, ad esempio, i formati PDF/H e XML HL7 per i documenti sanitari, PDF/B e PDF con caratteri interoperabili, DOTX, DOCX, XSLX, PPTX (staticizzati con profilo strict), ODT, HTML con restrizione, SQL.

Queste conseguenze, attentamente valutate dai conservatori stessi – che ne hanno, appunto, effettuato richiesta –, hanno indotto AgID a stabilire una proroga all'entrata in vigore delle LG, che diverranno efficaci il primo gennaio 2022[72].

[72] La relativa notizia, diffusa in data 18 maggio 2021, è pubblicata al link <https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/05/18/linee-guida-documenti-informatici-prorogata-data-entrata-vigore>.

II.3 I modelli e i progetti per la conservazione digitale

I Poli di conservazione

Già previsti nel Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019[1], i Poli di Conservazione[2] sono sistemi, realizzati dalle Pubbliche Amministrazioni col coordinamento dell'Archivio Centrale dello Stato, che consentono la conservazione a lungo termine dei propri archivi digitali; all'interno del documento si ponevano come obiettivi la messa a regime e l'utilizzo, da parte delle Pubbliche Amministrazioni, dei sistemi di conservazione a norma per tutti i propri documenti informatici e l'avvio di un percorso di adeguamento normativo utile ad assicurare che i servizi di conservazione garantissero la presenza sul territorio nazionale di almeno una copia operativa per ciascun documento informatico conservato.

Vengono poi nel Piano Triennale 2019-2021[3], che definisce ulteriori intenti di miglioramento riguardo ai Poli: l'adeguamento dei sistemi di conservazione perché siano abilitati a gestire tutte le possibili tipologie di documenti e oggetti digitali prodotti dalle PA, anche quelli soggetti a particolari criticità dal punto di vista della privacy e della sicurezza nazionale; la costituzione di un punto unico di accesso ai documenti informatici custoditi, per facilitare AgID e l'Archivio Centrale dello Stato nei loro compiti di vigilanza e ispezione sulla documentazione in conservazione e agevolare i cittadini e le imprese che hanno necessità di accedere ai documenti che la PA conserva per loro conto; la conservazione permanente della memoria della comunità nazionale e dello Stato, secondo quanto previsto

[1] *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019*, Agenzia per l'Italia Digitale, disponibile online al sito <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2017-2019/doc/01_piano-triennale-per-informatica-nella-pa.html>, pp. 49, 57.

[2] S. Pigliapoco, *Guida alla gestione informatica dei documenti*, Lucca, Civita editoriale, 2020, pp. 49-51; si veda anche la sezione dedicata *Poli di conservazione* sul sito istituzionale AgID al link <https://www.agid.gov.it/it/piattaforme/conservazione/poli-conservazione>. Si precisa sin d'ora che, tra gli scenari attualmente esistenti (Polo di conservazione dell'Archivio centrale dello Stato, Agenzia Industrie Difesa, Centro di Dematerializzazione e Conservazione Unico della Difesa, Consiglio Nazionale del Notariato, Società generale d'informatica S.p.A., Polo archivistico dell'Emilia-Romagna, Regione autonoma Friuli Venezia Giulia, Polo Marche DigiP-Regione Marche, Centro archivistico Regione Veneto, Polo della Regione Toscana), si scelgono come casi di studio il Polo archivistico dell'Emilia Romagna, il Polo Marche DigiP e Polo di conservazione dell'Archivio centrale dello Stato.

[3] *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021*, Agenzia per l'Italia Digitale, disponibile online al sito <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/index.html>, pp. 107-109.

dalle norme archivistiche. Si predilige, in questo documento, l'ottica di interoperabilità: vi si stabilisce di elaborare delle regole tecniche e normative finalizzate a definire le modalità interscambio dei pacchetti tra differenti sistemi di conservazione.

A tal proposito, AgID, dal 2019, ha attivato un tavolo di lavoro in coordinazione con l'Archivio centrale dello Stato, il Consiglio nazionale del notariato e l'Agenzia industrie difesa (cui si sono aggiunti, in seguito, Ministero dell'Economia e delle Finanze, Ministero della Giustizia, Direzione generale Archivi, Polo archivistico dell'Emilia-Romagna, Regione autonoma Friuli Venezia Giulia, Regione Marche, Regione Veneto, Società Generale d'Informatica S.p.A., Associazione Nazionale Archivistica Italiana): il documento *Progetto Poli di conservazione. Definizione di un modello di riferimento per i Poli di Conservazione e della relativa rete nazionale*[4], i cui lavori di abbozzo si sono chiusi il 3 maggio 2021, contiene una parte introduttiva e generale sugli archivi digitali, le modalità di conservazione a termine e permanente e i riferimenti normativi, una parte dedicata specificatamente ai Poli per la conservazione dei documenti e degli archivi informatici e al concetto di Rete dei Poli, una alle caratteristiche dei pacchetti e dello scambio di questi ultimi, perché siano leggibili e utilizzabili da diversi sistemi e, infine, la ricognizione accurata dei Poli già attivi[5].

Il documento parte dai problemi identificati in relazione alla conservazione permanente, tra cui la molteplicità di sistemi di archiviazione esistenti, le diverse esigenze di conservazione legate anche alle tipologie documentali, dalle diverse valorizzazioni dei corredi di metadati e dagli assetti amministrativi e tenta di fornire soluzioni che permettano una gestione uniforme della documentazione risultante dalle attività della Pubblica amministrazione, nell'ottica dell'interoperabilità a livello nazionale e finalizzata alla

[4] Il documento è stato pubblicato il 26 giugno 2021 (si veda, in proposito, la notizia al link <https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/06/23/poli-conservazione-pubblicato-il-documento-indirizzo> ed è consultabile online al sito <https://www.agid.gov.it/sites/default/files/repository_files/definizione_di_un_modello_di_riferimento_per_i_poli_di_conservazione_e_della_relativa_rete_nazionale_0.pdf>. È rivolto ai soggetti di cui all'art. 2 commi 2 e 3 del CAD.

[5] Le informazioni sul documento (oltre che dalla consultazione dello stesso) e sui Poli di conservazione citati a titolo di esempio sono state reperite attraverso gli interventi di Gabriele Bezzi, Serenella Carota, Patrizia Gentili, Maria Guercio, Silvia Trani, in occasione del seminario 'Poli archivistici di conservazione digitale', tenutosi il 3 maggio 2021 nell'ambito dei 'Lunedì del Master', ciclo di seminari organizzati nell'ambito del master di II livello 'Formazione, Gestione e Conservazione di Archivi Digitali in ambito pubblico e privato' (i materiali sono disponibili all'interno della pagina dedicata del sito del Master al link <https://www.masterarchividigitali.unimc.it/poli-archivistici-di-conservazione-digitale-03-05-2021-seminario-online-a-cura-di-mariella-guercio/>).

conservazione permanente, e che prevedano modalità di accesso semplici e unificate al patrimonio di *records* digitali. Tra i principi e i requisiti generali individuati a riguardo, è importante menzionare che è necessario concepire la conservazione non in relazione al singolo documento, ma con riferimento principale le aggregazioni documentali e le loro relazioni, al fine di preservare l'archivio nella sua unità; a tal proposito, è fondamentale disporre delle informazioni relative proprio all'ordinamento di questi ultimi e all'organizzazione del soggetto produttore stesso, per poter ricostruire il sistema originario di produzione; infine, si dispone che la custodia degli archivi pubblici venga presa in carico da istituzioni adeguatamente predisposte e che adottano procedure di produzione di copie autentiche che attestino in maniera certa la conformità, per la consapevolezza della difficoltà di preservare a lungo termine l'insieme di bit originario.

Per quanto riguarda i casi d'uso operativi, esistono diverse tipologie di Poli, differenziate per scopo e provenienza dei documenti: la prima è relativa alle realtà territoriali, di cui due esempi interessanti per via della lunga esperienza sono il Polo archivistico dell'Emilia-Romagna (ParER) e il Polo Marche DigiP.

Il primo, istituito nel 2009 nell'ambito dell'Istituto per i Beni Artistici, Culturali e Naturali della Regione Emilia-Romagna (IBACN) e accreditato come conservatore presso AgID nel 2014, è anche qualificato come fornitore di servizi SaaS[6] nel CloudPA. Sin dal 2010 ParER ha stipulato un accordo di collaborazione con la Soprintendenza archivistica per l'Emilia Romagna, che si occupa di vigilare sul processo di conservazione, perché questo avvenga in conformità alla normativa e nel rispetto della considerazione dei documenti come beni culturali[7].

L'Emilia-Romagna ha avviato uno dei tentativi più precoci di realizzare un sistema di conservazione regionale che fungesse da concentratore per tutte le altre amministrazioni locali (e oltre): a partire dal 2004, l'Emilia-Romagna si è distinta per le iniziative legate all'organizzazione dei processi di conservazione, per arrivare alla costituzione del Polo

[6] *Software as a Service*. Si definiscono SaaS i servizi forniti da un *provider* via cloud computing, che offre un'applicazione tramite browser web.

[7] Su ParER, si vedano il sito istituzionale del Polo archivistico della Regione Emilia Romagna <https://poloarchivistico.regione.emilia-romagna.it/>; A. Zucchini, *Il Polo archivistico regionale dell'Emilia-Romagna*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

archivistico: la struttura di questo sistema è complessa, proprio in ragione della molteplicità di enti di cui costituisce il riferimento, e si configura nel software SACER (Sistema per l'Archivio di Conservazione dell'Emilia Romagna). Questo, basato sul modello OAIS, propone i moduli base e i processi descritti dallo stesso standard, prevede la definizione di pacchetti di versamento che rappresentano specifiche aggregazioni, ovvero le Unità documentarie: queste sono le unità logiche elementari da cui è composto l'archivio, ovvero aggregati di uno o più documenti che sono da considerare come un solo oggetto (ad esempio, uno o più documenti principali – che possono anche essere semplicemente costituiti da soli metadati – con eventuali allegati o annotazioni; l'entità minima dell'archivio, invece, è l'Unità archivistica, che raccoglie le Unità documentarie. Gli oggetti sottoposti a conservazione in queste forme sono i documenti informatici, i documenti amministrativi informatici e le aggregazioni documentali informatiche, ciascuno con il proprio corredo di metadati; questi vengono versati in due fasi: la prima consiste nel versamento anticipato dei documenti, la seconda nel versamento in archivio delle aggregazioni: una volta verificati, i Pacchetti di Versamento diventano, in queste forme, Pacchetti di Archiviazione.

La modalità di impostazione del rapporto con gli enti versanti è costituita da due documenti fondamentali: l'Accordo e il Disciplinare tecnico; l'Accordo (il cui modello è concordato con la Soprintendenza Archivistica e Bibliografica dell'Emilia Romagna) consiste in una convenzione sottoscritta dalle parti, ovvero IBACN tramite ParER e il soggetto produttore e regola i rapporti di servizio tra il questo e l'IBACN, la natura dei servizi offerti, la responsabilità delle parti e le condizioni economiche, che vengono inserite soltanto per gli enti di altre regioni, in quanto l'erogazione dei servizi di conservazione per gli enti dell'Emilia-Romagna avviene a titolo gratuito. Il Disciplinare tecnico, invece, contiene le specifiche operative e le modalità di descrizione e di versamento dei documenti e delle aggregazioni.

Allo stato attuale, usufruiscono dei servizi ParER la Regione stessa e sue agenzie, trecentodieci Comuni, quarantuno Unioni di Comuni, nove Province e la Città Metropolitana di Bologna, trecentoventotto altri enti (ovvero tutte le Aziende ed enti del servizio sanitario regionale, l'Università di Bologna e diversi istituti scolastici), oltre che istituzioni al di fuori del territorio regionale.

Il Polo marchigiano è stato costituito nel 2010 e riconosciuto conservatore accreditato nel 2016: anch'esso basato sul modello OAIS, fornisce una soluzione tecnologica, organizzativa e archivistica per la conservazione di archivi digitali dell'Amministrazione regionale e degli enti locali del proprio territorio, ma anche per gli archivi digitali di soggetti privati e di altri soggetti pubblici come le aziende sanitarie[8]. L'architettura, più semplice rispetto a quella di ParER, si compone dei moduli previsti da ISO 14721 e prevede l'utilizzo del sistema di pacchetti in esso descritto, con una grande attenzione posta agli aspetti legati alle fasi di *ingest* e di *access* per facilitare l'esperienza dell'utente utilizzatore. Gli oggetti conservati sono costituiti da documento informatico, documento amministrativo informatico e aggregazioni, che siano fascicoli informatici e serie documentali, rappresentati in Unità documentarie, Unità archivistiche e Aggregazioni documentali informatiche. I PdV con Unità documentarie, una volta validati, sono trasformati in PdA; un PdV che contiene un'Unità archivistica o un'Aggregazione documentale informatica, invece, è finalizzato alla creazione di AIC.

In aggiunta, Marche DigiP include la possibilità di servirsi del software di protocollo e gestione documentale, interoperabile *by design* con il sistema di conservazione. L'organizzazione è distribuita in Unità di competenza formate da figure professionali specializzate, rispettivamente di Progettazione (dedicata alla pianificazione e alla consulenza in ambito archivistico, normativo e informatico e alla coordinazione delle altre Unità), di Gestione (attivo sull'implementazione del modello conservativo e sull'help desk) e di Data Center (deputato al corretto funzionamento e all'aggiornamento delle componenti tecnologiche).

È attivo, al fine di garantire un alto livello del servizio erogato, un Comitato scientifico, che si avvale anche di un tavolo regionale di *users* (il Comitato utilizzatori), che si occupa di definire la metrica su cui misurare la qualità, dell'approvazione del piano di audit e monitoraggio e degli aggiornamenti relativi a evoluzione tecnologica, normativa e standard,

[8] Su Marche DigiP, si vedano la sezione dedicata del sito istituzionale della Regione Marche <https://www.regione.marche.it/Regione-Utile/Agenda-Digitale/Polo-di-conservazione-regionale>; S. Carota, *Dematerializzazione: la strategia della Regione Marche* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

fornendo in tal modo supporto e integrazione all'Unità di progettazione che si occupa della redazione della documentazione e delle implementazioni.

I soggetti che intendono aderire al progetto per usufruire dei servizi del Polo Marche DigiP, sottoscrivono una convenzione e uno specifico disciplinare tecnico: la formula di copertura dei costi prevede la compartecipazione degli enti agli oneri a titolo di rimborso spese, nello specifico per la gestione operativa, i servizi di monitoraggio e assistenza agli enti produttori e i servizi di manutenzione del software.

Al momento, si avvalgono del servizio Marche DigiP duecento otto Comuni, quattordici Unioni dei Comuni e Unioni Montane, ventidue Enti (Regione Marche, Assemblea Legislativa Regione Marche, Province, Aziende sanitarie, Aziende di servizi pubblici, enti regionali, ecc.).

La seconda tipologia di Poli è relativa alle amministrazioni centrali: un esempio è il Consiglio nazionale del Notariato[9]. La piattaforma sviluppata da Notartel, accreditata come conservatore da AgID nel 2016, è disponibile esclusivamente per i notai, ed è attivabile per due distinte funzioni: la prima consente di conservare a norma gli atti per cui non esiste un obbligo effettivo di mantenimento, mentre il secondo è dedicato alla documentazione fiscale.

Per il terzo tipo, connesso alla conservazione permanente, è in corso di sviluppo il progetto costituzione del Polo di conservazione dell'Archivio centrale dello Stato (PCACS).

Innanzitutto, ha un impostazione differente dai casi già discussi in quanto all'ACS è demandata istituzionalmente la custodia permanente della documentazione degli organi centrali dello Stato, nonché di soggetti privati che risultino di interesse storico. Le attività sono cominciate nel 2019, con l'avvio delle valutazioni preliminari, che hanno evidenziato le difficoltà connesse alla conservazione degli oggetti digitali che confluiscono da sistemi su cui l'ACS non ha competenza; altra questione emersa riguarda la tipologia di oggetti da porre effettivamente in conservazione, dal fascicolo alla banca dati, dai siti web alle evidenze dei social network; altro punto focale della riflessione ha riguardato la diversità dei regimi di

[9] In proposito, si vedano il sito della Società informatica del notariato italiano al link <https://www.notartel.it/notartel/contenuti/servizi/paDigitale/can.html# >; A. Mazzeo, M. Nastri, *Aspetti tecnici e organizzativi della conservazione: il caso del Notariato italiano,* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

accesso alla documentazione custodita, che si differenzia a seconda dei documenti raccolti; l'ultimo punto è relativo al modello organizzativo per la conservazione: si è scelto di sviluppare la piattaforma *in house*, ma si è scelto di affidarsi a un'infrastruttura esterna. Relativamente ai modelli, ci si è riferiti a Archivematica e eARK[10], al fine di attingere da strumenti e processi sviluppati in ambito internazionale da poter adattare alle proprie esigenze. In particolar modo, si è preso ad esempio il pacchetto informativo di eARK e lo si è adeguato alle caratteristiche di cui l'ACS ha necessità. Per dare forma agli effettivi strumenti d'uso è in corso la sperimentazione: si sta verificando il modello organizzativo funzionale, si stanno testando le componenti, si stanno impostando i criteri di vaglio e rilevazione dei sistemi di gestione documentale, si sta proseguendo la tipizzazione degli oggetti digitali da sottoporre al processo di conservazione e si sta consolidando una rete nazionale di referenti dai diversi profili e obiettivi.

Standard internazionali e nazionali

Dal quadro delineato nel precedente paragrafo emerge l'ampio ricorso a standard internazionali e nazionali, con la finalità di conferire ai sistemi di conservazione determinate caratteristiche organizzative, di qualità e architetturali. La norma, prevedendo la triplice possibilità di sviluppare sistemi di conservazione *in house*, di affidare il servizio a soggetti terzi e di adottare soluzioni miste, prescrive la conformità a standard che ne descrivano le modalità di realizzazione, che ne garantiscano la sicurezza fisica e logica e che ne incrementino l'interoperabilità.

Nelle Linee Guida AgID[11] sono citati gli standard UNI SInCRO[12], ISO/IEC 27001, ISO 14721 e le raccomandazioni ETSI TS 101 533-1[13].

[10] Su Archivematica e eARK si veda il capitolo I.3.

[11] Come si è già esposto nel capitolo II.2, i richiami agli standard sono i medesimi della normativa precedente in materia di accreditamento.

[12] Linee Guida AgID, par. 4.2 «[..] L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali».

[13] Linee Guida AgID, par. 4.3 Modelli organizzativi «[..] Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems - Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione

UNI SInCRO[14], il cui primo rilascio risale al 2010 e il cui aggiornamento è stato emesso nel 2020, descrive, in conformità con il disegno dei pacchetti OAIS, la struttura dell'insieme di dati a supporto del processo di conservazione e recupero degli oggetti digitali, individuando gli elementi informativi necessari alla creazione dell'indice di conservazione (denominato anche 'file di chiusura') e descrivendone sia la semantica sia l'articolazione attraverso il linguaggio formale XML.

Il corpo principale del documento è organizzato in tre sezioni: la prima descrive la struttura del 'file di chiusura', comprensiva della rappresentazione formale, la seconda contiene *la tag library*, con la spiegazione di elementi e attributi, la terza degli esempi di utilizzo. Nella sua versione originaria lo standard prevedeva, per la costruzione del 'file di chiusura', una struttura ad albero composta dalle radici 'Self description', 'VdC', 'FileGroup' e 'Process': questi, rispettivamente descrizione dell'indice, unità logica elementare composta da uno o più file, dall'indice di conservazione e dagli indici di conservazione antecedenti (se l'indice di conservazione attuale è stato originato da questi), rappresentazione del contenuto e processo di conservazione cui è stato sottoposto, sono caratterizzati da ulteriori elementi subordinati, che ne identificano le caratteristiche.

Con l'entrata in vigore delle Linee Guida AgID, se ne avrà un effettivo obbligo di adozione per tutte le tipologie di conservatori: in precedenza, infatti, il DPCM 3 dicembre 2013 (C) individua lo standard nell'allegato 3 come raccomandato, mentre nell'allegato 4 delinea una struttura per l'IPdA basata su SInCRO ma non del tutto uniforme rispetto a questo. In seguito, si è provato ad arginare il problema con l'inserimento di UNI SInCRO nell'ambito dei vincoli per la qualifica di conservatore accreditato nel documento *Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza*, per cui la conformità a UNI SInCRO è una condizione *sine qua non* per ottenere la certificazione come conservatore

---

e ISO 14721 OAIS (*Open Archival Information System - Sistema informativo aperto per l'archiviazione*), e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni*». Non si trattano, in questo paragrafo, i già menzionati ISO 14721 e le raccomandazioni ETSI TS 101 533-1 (si rimanda, in proposito, al capitolo I.2); si descrivono, invece, UNI SInCRO e ISO/IEC 27001.

[14] Lo standard è disponibile al link <http://store.uni.com/catalogo/uni-11386-2020?josso_back_to=http://store.uni.com/josso-security-check.php&josso_cmd=login_optional&josso_partnerapp_host=store.uni.com> (l'accesso è vincolato al pagamento della risorsa). Su UNI SiNCRO si veda G. Michetti, *Lo standard UNI SInCRO: un supporto alla conservazione digitale*, «Archivi & Computer», 1 (2011), San Miniato, pp. 40-53.

accreditato; proprio per tale ragione, però, è un vincolo che riguardava solo i soggetti che intendevano conseguire l'accreditamento AgID e che, soprattutto, era ancorato a un documento che non è propriamente ascrivibile alla categoria dei provvedimenti di legge, poiché non presenta alcuna firma, non costituisce un allegato e l'ufficialità è data soltanto dalla pubblicazione sul sito istituzionale dell'AgID.

Il rilascio di UNI 11386:2020, sostanzialmente, non determina un adeguamento dei file di chiusura già in conservazione rispetto alla nuova versione dello standard. Riguardo alla struttura dell'Indice di Conservazione, è da sottolineare che, pur essendo sostanzialmente la stessa, presenta più elementi e si è data una maggior possibilità di descrizione di questi ultimi: l'obiettivo è rendere lo standard il più autoesplicativo possibile, per favorire l'interoperabilità e lo scambio di informazioni tra sistemi; inoltre, come novità, i tag sono per la maggior parte in lingua inglese, per un'auspicata adozione a livello europeo, il nome del file che contiene l'indice ha un nome costruito con 'Pindex', seguito dall'identificativo alfanumerico e dall'estensione, e il tag 'Agent' ha una nuova configurazione: si noti l'aggiunta dell'elemento 'RelevantDocument', ovvero l'obbligo di indicare almeno un documento che giustifica che ruolo abbia l'Agent, come il Manuale di conservazione o di gestione. Nella tag library, oltre ai dettagli già presenti nella versione 2010, sono state aggiunte le indicazioni operative su come utilizzare in concreto un dato tag, compresa l'indicazione di eventuali altri standard di riferimento, le definizioni sono semplificate, grazie all'utilizzo dei campi 'Regole sintattiche' e 'Note' per le indicazioni operative: le funzioni essenziali restano le stesse, ma si è tentato di correggere ambiguità interpretative e di esplicitare i riferimenti normativi[15].

ISO/IEC 27001:2013 *Information technology – Security techniques – Information Security Management Systems – Requirements*[16], prescritto nelle Linee Guida AgID e già collocato tra le certificazioni obbligatorie da conseguire per l'accreditamento, fa parte della famiglia di standard ISO 27000, dedicati alla gestione della sicurezza delle informazioni, da quelle finanziarie, connesse alla proprietà intellettuale, contenenti dati personali o affidate da terze parti. Nello specifico, la norma 27001 è concepita come certificabile e fornisce i

[15] L'analisi comparativa tra le versioni di UNI SInCRO è stata effettuata nell'ambito delle attività svolte presso l'azienda Namirial S.p.A.: ne è risultato il documento interno *Confronto versioni UNI SInCRO 2010 – UNI SInCRO 2020*, redatto con il Responsabile della funzione archivistica Enrico Giunta.

[16] Lo standard è disponibile al link <https://www.iso.org/isoiec-27001-information-security.html> (l'accesso è vincolato al pagamento della risorsa).

requisiti necessari all'implementazione, al monitoraggio e al miglioramento continuo di un Sistema di gestione della sicurezza delle informazioni (ISMS) nel contesto di un'organizzazione: include, a tal proposito, requisiti per la valutazione e il trattamento dei rischi per la sicurezza delle informazioni, tarati sulle esigenze del singolo ente o impresa; quanto indicato, infatti, è formulato appositamente per essere applicato ad ogni genere di organismo o azienda, indipendentemente dal tipo, dalle dimensioni o dalla natura. Al fine di conseguire la certificazione ISO 27001, è necessario fare riferimento all'Annex A dello standard: questo contiene la matrice dei controlli da verificare, che corrispondono alle aree in cui è suddiviso il testo del documento, ovvero: *Context of the* organization, in cui viene definito che l'organizzazione deve determinare, sulla base delle contingenze interne ed esterne, lo scopo, i confini e l'applicabilità dell'*Information Security Management System* (ISMS); *Leadership,* in cui si afferma che l'apparato dirigente debba assicurare, attraverso un coinvolgimento costante, che le *policies* di sicurezza siano implementate e che vi sia una struttura di ruoli con relative responsabilità che garantisca il funzionamento del sistema e il rispetto delle regole; *Planning,* che contiene i requisiti di pianificazione in relazione a valutazione del rischio e prevenzione di incidenti; *Support,* in cui si dichiara che l'organizzazione deve possedere le risorse necessarie, con le opportune competenze e conoscenze, per l'istituzione, l'implementazione, la manutenzione e il miglioramento continuo dell'ISMS; *Operation,* in cui si raccomandano la programmazione, la realizzazione e il controllo dei processi volti a soddisfare i requisiti di sicurezza delle informazioni e alla disposizione della documentazione finalizzata a dimostrare l'efficacia e la messa in atto di tali processi e l'idoneità di eventuali modifiche; *Performance evaluation* e *Improvement,* in cui si dichiara che l'organizzazione debba monitorare e misurare l'efficacia di quanto implementato, attraverso attività di *internal audit* e *management review*, allo scopo di conseguire un miglioramento continuo ed efficienza nell'individuazione celere delle non conformità e nella loro correzione. Questa checklist di riscontro può essere utilizzata tanto da organismi valutatori esterni, per poter ottenere l'effettiva certificazione, quanto internamente, per procedure di audit interni e su terze parti.

In aggiunta a queste norme, nel Regolamento sui criteri per la fornitura dei servizi di conservazione, sono inseriti ISO 16363, ETSI EN 319 401 («con l'adozione di criteri

derivanti dallo standard ETSI TS 119 511 e da tutte le norme richiamate applicabili»[17]) ISO 37001, ISO 9001 e ISO/IEC 22313[18].

ISO 37001:2016 *Anti-bribery management systems – Requirements with guidance for use*[19] è uno standard certificabile che consente alle organizzazioni di prevenire, individuare e gestire i tentativi di corruzione, adottando *policies* che prevedono il conferimento, a un membro dello staff, dell'incarico di supervisionare la conformità alla legge, la formazione, le valutazioni del rischio e la *due diligence* su progetti e soci, implementando controlli finanziari e commerciali e istituendo procedure di segnalazione e indagine. ISO 37001 fornisce un modello flessibile e adattabile a diverse realtà, che specifica come affrontare la corruzione nei settori pubblico, privato e no-profit interna all'organizzazione stessa, perpetrata dal personale interno che agisce per conto dell'impresa o ente interessato o a suo beneficio, da partner e soci, diretta e indiretta.

Le misure richieste da ISO 37001 sono progettate per essere integrate con i processi di gestione e i controlli esistenti: segue, infatti, la struttura di alto livello comune per gli standard dei sistemi di gestione ISO, per una facile integrazione con, ad esempio, ISO 9001. La norma definisce genericamente il termine 'corruzione' in quanto ogni apparato normativo nazionale prevede la propria e il suo trattamento dipenderà dalle leggi applicabili all'organizzazione e, seguendo questa logica, delinea requisiti minimi e linee guida di supporto per l'implementazione o il *benchmarking* di un sistema di gestione anti-corruzione: la sua certificazione costituisce prova del fatto che, presso l'organizzazione, è in vigore una definita politica anti-corruzione, che comprenda azioni correttive e prospettive di miglioramento, che vi sia il commitment e la responsabilità del management, che il personale venga controllato

[17] Allegato A *Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni* al *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*, RG7; l'RG6 specifica che «Fino al 31/12/2022, il servizio erogato dovrà essere conforme allo standard ETSI TS 101 533-1, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni. Il requisito del supporto della TS 101 533-1 si considera soddisfatto se il conservatore è conforme alla TS 119 511».

[18] Allegato A *Requisiti per l'erogazione del servizio di conservazione per conto delle pubbliche amministrazioni* al *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*, RG3-RG7, RG9, RQ1, RS1, RS3. Analogamente a quanto dichiarato in nota 13, non si trattano, in questo paragrafo, i già menzionati ISO 16363, ETSI EN 319 401 ed ETSI TS 119 511 (si rimanda, in proposito, al capitolo I.2); si descrivono, invece, ISO 37001, ISO 9001, ISO/IEC 22313.

[19] Lo standard è disponibile al link <https://www.iso.org/standard/65034.html> (l'accesso è vincolato al pagamento della risorsa).

e formato, che siano effettuate valutazioni dei rischi, controlli finanziari, commerciali e contrattuali anche su progetti e partner, che siano definite modalità di segnalazione, monitoraggio, indagine e revisione,

ISO 9001:2015 *Quality management systems - Requirements*[20], parte della famiglia ISO 9000, che affronta vari aspetti della gestione della qualità e fornisce un modello da seguire nella creazione e nel funzionamento di un sistema di gestione. Questo standard stabilisce i criteri per un sistema di gestione della qualità ed è l'unico della famiglia che può essere certificato: si basa su una serie di principi volti a garantire una forte attenzione al cliente, inclusione e reattività del *top management* e il miglioramento continuo. La norma specifica requisiti generici e applicabili a qualsiasi contesto per un sistema di gestione della qualità per le organizzazioni che necessitano di dimostrare la propria capacità di fornire prodotti e servizi che soddisfino i clienti e i requisiti legali e normativi applicabili. Nello specifico, con la consueta impostazione degli standard ISO nelle aree in Contesto dell'organizzazione, Leadership, Pianificazione, Supporto, Attività operative, Valutazione delle prestazioni e Miglioramento, si propone la valutazione di tutte le aree decisionali e operative e delle attività compiute, a partire dalla pianificazione generale sino alla consegna finale del prodotto o all'erogazione effettiva del servizio all'utente.

Viene proposta nel Regolamento, in alternativa a quella ISO 9001, la certificazione ISO/IEC 20000-1:2018 *Informatione tecnology – service management – service management system requirements*[21]: similmente alla norma 9001, questo documento specifica i requisiti per realizzare, monitorare e migliorare un sistema di gestione dei servizi (*service management system* – SMS), che includono la pianificazione, la transizione ad altri sistemi e la fornitura, per assicurare garanzie di qualità sui servizi e sulla capacità dell'organizzazione che li eroga di avviare attività di progettazione, di 'misurare' l'efficacia del SMS utilizzato e di attuare strategie finalizzate all'*improvement* continuo.

Il fornitore di servizi, per conformarsi al Regolamento, deve specificare inoltre l'applicazione delle *best practices* contenute in ISO 22313:2020 *Security and resilience* –

[20] Lo standard è disponibile al link <https://www.iso.org/standard/62085.html> (l'accesso è vincolato al pagamento della risorsa).

[21] Lo standard è disponibile al link < https://www.iso.org/standard/70636.html> (l'accesso è vincolato al pagamento della risorsa).

Business continuity management systems – Guidance on the use of ISO 22301[22]: questo documento fornisce una guida e delle raccomandazioni per l'applicazione dei requisiti del *business continuity management system* (BCMS) descritto nello standard ISO 22301. È applicabile a organizzazioni che implementano e monitorano un BCMS, che cercano di garantire la conformità con la politica di continuità aziendale dichiarata e che devono essere in grado di continuare a fornire prodotti e servizi a una capacità predefinita accettabile nel caso di interruzioni impreviste.

La guida e le raccomandazioni sono applicabili a tutti i tipi di organizzazioni, dalle piccole e grandi imprese al settore pubblico, seguendo un approccio scalato sull'ambiente operativo e sulla complessità del singolo soggetto.

[22] Lo standard (la cui versione è stata confermata nel 2021) è disponibile al link < https://www.iso.org/standard/75107.html> (l'accesso è vincolato al pagamento della risorsa).

Parte III. I casi di studio

III.1 Ambito, criteri e metodologia della descrizione dei casi di studio

L'indagine che si presenta consiste nella rilevazione del contesto istituzionale, della normativa, degli strumenti e dei modelli inerenti alla conservazione digitale di quattro Stati europei: Austria, Francia, Olanda e Romania. Lo scopo di tale approfondimento è poter effettuare un'analisi comparativa rispetto all'ambito italiano, al fine di evidenziare fattori comuni, punti di forza, elementi di diversità e caratteri di difformità e di impostare una riflessione organica[1].

L'inquadramento del tema, ai fini del reperimento delle informazioni, è molto complesso: come si è evidenziato nei precedenti paragrafi sul contesto europeo e italiano[2], la conservazione digitale consiste in principi e prassi che non solo si intersecano con diversi settori trasversali, ma sono oggetto di intenti amministrativi, politici e storico-culturali[3]. Ripercorrendo brevemente alcuni punti già messi in evidenza, al fine di richiamare delle premesse necessarie alla successiva descrizione dei contesti, va ricordato che, in primo luogo, è un ambito legato al dominio dell'archivistica: questa disciplina marca i confini tra lo stadio corrente degli archivi e il loro divenire, una volta trascorsa la fase intermedia, memoria storica. La conservazione digitale, dunque, interessando le fasi che seguono al passaggio all'"inattività" dei documenti, si colloca tra gli ambiti normati dalle leggi sulla formazione, gestione e conservazione della documentazione amministrativa[4] e dal diritto civile e privato, per i criteri sul valore probatorio del documento informatico.

[1] L'analisi comparativa vera e propria, con le relative considerazioni su ciascun contesto, verrà illustrata dettagliatamente nella Parte IV. In questa sede ci si limita al fotografare le realtà selezionate, al fine di fornire una panoramica funzionale all'analisi critica e di confronto che verrà esposta, come già affermato, nella Parte IV.

[2] Si vedano, in proposito, i capitoli. I.1 e II.1.

[3] Si pensi agli aspetti legati alle Agende nazionali per la digitalizzazione: i servizi di archiviazione elettronica e di consultazione si inseriscono nei piani per l'informatizzazione e lo sviluppo tecnologico delle pubbliche amministrazioni e sono compresi negli ambiti d'azione degli organismi preposti alla supervisione e alla realizzazione di questi obiettivi.

[4] Vista la finalità introduttiva di questa sezione e il riferimento a una pluralità di contesti normativi, non si citano, in questa sede, degli esempi di provvedimenti: si rimanda, per l'approfondimento di questi ultimi, alla trattazione dei casi specifici nei paragrafi che seguono.

Va tenuto conto anche dell'eterogeneità del contenuto degli archivi. È rilevante, infatti, anche la disciplina giuridica in materia di dati personali, fiscale e commerciale: oltre agli aspetti legati alla conservazione 'in sé', è necessario tenere in considerazione gli aspetti intrinseci del materiale da conservare ed effettuare valutazioni in base alla normativa che ne determina la gestione e la tenuta[5].

Inoltre, data la natura di beni culturali dei documenti informatici prodotti dalla Pubblica amministrazione e dai soggetti privati di interesse storico, questi sono sottoposti ai provvedimenti emanati a tutela del patrimonio storico e culturale.

Infine, vi è l'ambito tecnologico: se, da un lato, si cerca di non vincolare in maniera mandatoria ciò che è maggiormente soggetto a evoluzione e aggiornamenti, dall'altro si deve intervenire in maniera decisiva sulla sicurezza informatica e alla robustezza delle infrastrutture.

Scendendo nel dettaglio degli Stati esaminati, è innanzitutto necessario chiarire le motivazioni della selezione: questa si basa su criteri volti a consentire la disposizione di un campione diversificato da diversi punti di vista. Innanzitutto, si è cercato di prendere a esempio nazioni con ordinamenti giuridici differenti: vista la stretta correlazione tra le regolamentazioni di ambito archivistico e l'assetto istituzionale statale, si è scelto di rappresentare nell'analisi repubblica parlamentare di tipo federale[6], repubblica semipresidenziale[7] e monarchia parlamentare[8]. Si è, inoltre, tentato di privilegiare contesti con una 'storia' e un background archivistico differente[9].

Le attività accademiche frequentate a livello internazionale hanno, poi, determinato la focalizzazione su alcune realtà particolarmente operative e attente allo sviluppo delle

[5]Questi aspetti non sono oggetto di approfondimento nella rilevazione dei contesti e dell'analisi comparativa, in quanto, sebbene costituiscano il livello 'operativo' sottostante ai processi di conservazione e l'oggetto di determinate scelte conservative (anche dal punto di vista contrattuale, nel caso si affidi il servizio in *outsourcing*), renderebbe indispensabile un *deep-dive* sulle discipline giuridiche e un'analisi della normativa di settore non adeguate rispetto al tema del presente elaborato. Si illustrano casi particolari che toccano queste contingenze soltanto nei casi in cui le disposizioni di settore svolgano una funzione integrativa rispetto a quelle generali.

[6] Austria.

[7] Francia e Romania.

[8] Olanda.

[9] A riguardo, si accennano le vicende degli Archivi di Stato e degli Archivi Nazionali, per una comprensione più compiuta del contesto attuale.

innovazioni e al progresso nel campo della conservazione digitale e il conseguente interesse per l'approfondimento del panorama normativo specifico[10]. Infine, incidendo nel progetto anche l'elemento aziendale - vista la già citata tipologia EUREKA del progetto - la scelta è sensibile anche alle esigenze di ricerca applicata: si è provveduto all'esame di realtà simili all'Italia dal punto di vista normativo, per poter ampliare gli orizzonti commerciali[11].

Dunque, si è dovuto procedere con il reperimento delle informazioni attraverso diversi canali, attivi su più piani. In primo luogo, si è provveduto all'individuazione di strutture e figure da contattare per collezionare notizie sugli aspetti normativi e i modelli adottati: per questa prima fase di indagine, ci si è rivolti principalmente agli Archivi Nazionali e agli organismi statali operanti in materia di digitalizzazione. Disponendo, inoltre, della possibilità di fare riferimento a figure professionali delle sedi estere di Namirial S.p.A.[12], si sono raccolte informazioni attraverso gli apparati direzionali e commerciali di queste filiali operative.

Una volta vagliati i riferimenti generali rintracciati, si sono analizzati i siti web istituzionali degli organi governativi contenenti le indicazioni e i dettagli specifici inerenti ai provvedimenti legislativi di settore, alle norme operative, agli standard e ai progetti messi in atto per garantire un riscontro diretto a questi strumenti dispositivi[13]; ove necessario, si sono consultati anche i siti web delle aziende che forniscono servizi di conservazione aventi sede legale nello Stato d'interesse.

Infine, la raccolta dei dati si basa anche sulle informazioni tratte dalla frequenza a convegni e seminari, sui contatti con i relatori, nonché dalla consultazione dei riferimenti e

[10] È il caso di Francia e Olanda che, come si vedrà nei capitoli III.3 e III.4, mostrano una particolare concomitanza tra formulazione di leggi e sviluppo della ricerca applicata.

[11] È il caso di Austria e Romania. Si menziona, in questa sede, che quanto prodotto in ambito aziendale riguardo all'analisi comparativa è lavoro a quattro mani compiuto con la dottoressa Margherita Menghini, tutor aziendale per il presente progetto di ricerca e Auditor interno TSP presso Namirial S.p.A.

[12] Austria (Namirial GmBH) e Romania (Namirial S.r.l.).

[13] A questo proposito, si pongono in rilievo due considerazioni. In primo luogo, la varietà delle lingue di redazione dei dispositivi normativi e dei contenuti online ha determinato il ricorso a strumenti di traduzione automatica, integrati da valutazioni di esperti soltanto nei casi di interpretazioni controverse. Si precisa, in questa sede, che, ove possibile, si sono menzionati e termini denominazioni in lingua originale, mentre la normativa citata in maniera testuale è esposta in traduzione italiana. Inoltre, dal momento che i *framework* normativi sono in costante evoluzione per la rapida evoluzione tecnologica e l'affacciarsi di nuove problematiche e soluzioni, è importante l'anno di riferimento di ciascun provvedimento: sebbene si sia prestata molta attenzione all'aggiornamento costante, nell'elaborato potrebbero non risultare gli emendamenti posteriori al momento della stesura e delle ulteriori revisioni.

dei materiali online relativi alle associazioni e agli organismi che si occupano della loro organizzazione.

Viste tali modalità di reperimento dei dati, si è scelto di citare le strutture e le figure contattate che hanno fornito informazioni e fonti bibliografiche nella nota di incipit di ciascun paragrafo relativo all'analisi di ogni Stato e di dotare l'elaborato di un appendice contenente i siti istituzionali consultati[14].

Per quanto riguarda la struttura dell'analisi di ciascuna realtà nazionale, si fornisce un inquadramento generale del contesto istituzionale in cui si collocano le competenze sulla conservazione digitale: si menzionano gli enti governativi che sovrintendono l'amministrazione degli archivi e degli organismi preposti al coordinamento della digitalizzazione, in quanto determinanti per la comprensione degli argomenti trattati di seguito.

Si presentano, poi, le disposizioni specifiche sulla conservazione digitale e gli archivi digitali, dai provvedimenti *ad hoc* ai dispositivi normativi integrativi rintracciati in normativa di argomento generale o di altro settore[15]. Si sottolinea che, ove possibile, si è scelto (e tentato) di conservare la terminologia riscontrata nelle fonti normative stesse: l'obiettivo è quello di salvaguardare le peculiarità di ciascun contesto, anche nei casi in cui si discostino dal lessico utilizzato in Italia.

Infine, si sono approfonditi i modelli di conservazione adottati in adempimento dei requisiti di legge e gli standard e le norme operative emessi per rispondere alle esigenze della conservazione a lungo termine, insieme ai documenti di indirizzo, alle iniziative e ai progetti avviati al fine di disporre di strumenti condivisibili e scalabili.

[14] Si veda l'Appendice A. Siti istituzionali consultati.

[15] I riferimenti normativi in nota non si normalizzano sulla base della consuetudine italiana, ma sono espressi secondo il metodo utilizzato nell'ambito della nazione in cui sono prodotti.

III.2 Austria[1]

III.2.1 Introduzione

La premessa necessaria per descrivere il funzionamento del 'sistema archivistico' austriaco è far riferimento alla sua forma di governo, la repubblica federale. Questo, infatti, implica che la gestione dei documenti avvenga su due livelli: la documentazione prodotta dalla federazione è sottoposta alle disposizioni sugli archivi federali, mentre i *records* prodotti dagli stati federati sono gestiti sulla base dei regolamenti degli archivi degli stati federali[2].

A livello di federazione, il controllo sulla conservazione dei documenti prodotti dagli enti e dagli uffici governativi è molto centralizzata e affidata, principalmente, alle competenze dell'Archivio di Stato austriaco e delle sue sedi territoriali.

Non si trovano, nel corpus normativo austriaco, disposizioni specifiche inerenti alla conservazione della documentazione digitale della federazione: nonostante ciò, *Österreichisches Staatsarchiv* e autorità competenti in materia di digitalizzazione avviano progetti e attuano *best practices* che permettono di adeguarsi alle esigenze di tenuta a lungo termine del materiale digitale. A riguardo è stato implementato DigLA, ovvero un sistema che consente la conservazione della documentazione prodotta o riprodotta elettronicamente dagli apparati statali.

Infine, riguardo all'attività dei privati nel settore, il ministero cui afferisce il tema della progressiva digitalizzazione dell'Austria, ovvero il *Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt*, ha avviato l'iniziativa *Ö-Cloud Gütesiegel*, che consiste nella possibilità, per i fornitori, di certificare i propri servizi erogati in modalità cloud.

---

[1] La bibliografia e le risorse telematiche per il contesto francese sono state reperite attraverso i contatti con Jonas Ruben Kerschner, Responsabile del dipartimento Archivio Digitale e Servizi IT presso la Cancelleria federale, Klaus Fellner, Head of sales and presales EMEA and APAC presso Namirial GmBH e Sergio Sette, IT & Digital Transformation consultant. Si segnalano, inoltre, i riferimenti dei principali siti web istituzionali consultati: sito istituzionale del *Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt* <https://www.bmdw.gv.at/>, *Digital Austria* < https://www.digitalaustria.gv.at/>, Sito istituzionale dell'iniziativa *Ö-Cloud-Gütesiegel* <https://oe-cloud.eurocloud.at/>, sito istituzionale *Österreichisches Staatsarchiv* <https://www.oesta.gv.at/>.

[2] In questo capitolo si descrive esclusivamente il contesto della federazione, in quanto la trattazione è finalizzata all'analisi comparativa dei requisiti generali in materia di conservazione digitale.

III.2.2 Conservazione digitale e contesto amministrativo: organismi preposti al coordinamento delle politiche sugli archivi

Gli organismi che esercitano competenze sulla gestione e sulla conservazione centralizzata dei *records* amministrativi digitali sono l'*Österreichisches Staatsarchiv* (Archivio di Stato austriaco) e il *Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt* (Ministero federale per la digitalizzazione e gli affari economici).

Österreichisches Staatsarchiv

L'autorità che sovrintende la gestione della documentazione della cancelleria federale è l'Archivio di Stato austriaco[3], che a essa è formalmente sottoposto. È l'archivio centrale per gli uffici federali, che devono trasferirvi gli atti e documenti relativi a pratiche concluse: in particolare, l'*Archiv der Republik* (Archivio della Repubblica) è il dipartimento dell'Archivio di Stato responsabile della valutazione, dello scarto, della presa in carico, della conservazione, della tenuta in sicurezza, della descrizione e della fruibilità per utenti e ricercatori del patrimonio archivistico. Oltre alla conservazione dei documenti analogici, sono trattati anche i materiali d'archivio in formato elettronico, ai fini del loro mantenimento a lungo termine e della loro accessibilità.

Dal punto di vista organizzativo, l'Archivio di Stato austriaco è un organo federale che riferisce direttamente al Cancelliere federale, il quale ne determina l'organizzazione interna, mentre la sua gestione è demandata al Direttore generale[4].

L'organizzazione complessiva e i compiti scientifici, culturali e amministrativi dell'Archivio di Stato austriaco sono definiti dalla *Bundesgesetz über die Sicherung,*

[3] L'Archivio di Stato austriaco ha origini che risalgono sino al Sacro Romano Impero (il più antico documento custodito risale all'819 d.C.), ma l'avvenimento nella storia recente a cui è necessario far riferimento per ricostruirne l'assetto attuale è la riorganizzazione a seguito dell'unificazione con la Germania: l'Archivio di Stato austriaco diviene la branca di Vienna dell'Archivio Centrale di Germania. Al termine della Seconda Guerra Mondiale, il governo austriaco riassume il controllo del proprio archivio nazionale, che sostanzialmente mantiene la sua conformazione, con una struttura organizzativa modificata. Nel 1983 viene creato l'Archivio della Repubblica, che diventa responsabile di tutti i *records* archivistici prodotti dagli uffici centrali della Repubblica d'Austria dalla sua fondazione nel 1918 e presso il quale, dunque, vengono versati tutti i documenti governativi da conservare; le altre sezioni diventano archivi storici. (P.C. Franks – A. Bernier Anthony (a cura di) *The international directory of national archives*, Lanham, Rowman & Littlefield, Lanham, 2018, pp. 23-25).

[4] § 12 [1;2], *Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz). StF: BGBl. I Nr. 162/1999.*

Aufbewahrung und Nutzung von Archivgut des Bundes (Legge federale sulla tutela, la conservazione e l'utilizzo degli archivi federali)[5]: questa inquadra come funzioni principali dell'Archivio di Stato austriaco il registrare, prendere in consegna, gestire, conservare, curare, ordinare, indicizzare, utilizzare e rendere fruibili i documenti d'archivio della Federazione per ricerche storiche e sul presente, per altre esigenze e ragioni scientifiche, per motivazioni legate alla normativa, alla giustizia e all'amministrazione, così come per legittimi interessi dei cittadini[6]. Dunque, l'Archivio di Stato austriaco, riveste il 'ruolo' di archivio di deposito e storico: oltre alle sue responsabilità chiave per gli studi della documentazione *ex post*, svolge anche compiti importanti per le attività in corso per l'amministrazione pubblica.

Oltre all'Archivio di Stato austriaco come archivio federale centrale e alle sue sedi territoriali deputate alla raccolta di documenti dei relativi uffici dipartimentali, altri dipartimenti e istituzioni federali sono autorizzati a formare i propri archivi con il materiale scritto prodotto dagli uffici che vi operano: la Direzione Parlamentare, le corti supreme, le università, l'Ufficio federale dei monumenti, la Biblioteca Nazionale Austriaca, i musei federali, la fonoteca austriaca, la banda musicale di corte e l'Ufficio federale di metrologia e topografia[7].

I servizi federali che non sono autorizzati a tenere un proprio archivio devono consegnare all'Archivio di Stato austriaco la documentazione che non è più necessaria per la gestione degli affari correnti, il quale, poi, ha facoltà di decisione sul valore culturale e archivistico di ciò che è versato. Per i materiali archivistici depositati presso l'Archivio di Stato sulla base di un accordo di deposito, si applicano condizioni speciali.

L'Archivio di Stato austriaco è, infine, l'autorità preposta della protezione dei documenti d'archivio secondo la Legge sulla protezione dei monumenti[8] e, in quanto tale, dà disposizioni sulla tutela di questa categoria di beni culturali nazionali e vigila contro il trasferimento illegale all'estero.

---

[5] Si veda, in proposito, il successivo paragrafo III.2.3.
[6] § 2 [5] *Bundesarchivgesetz BGBl. Nr. 162/1999*.
[7] § 3 [2] *Bundesarchivgesetz BGBl. Nr. 162/1999*.
[8] § 24-25 [1;2] *Bundesgesetz betreffend den Schutz von Denkmalen wegen ihrer geschichtlichen, künstlerischen oder sonstigen kulturellen Bedeutung (Denkmalschutzgesetz - DMSG) BGBl. Nr. 533/1923*.

L'Archivio di Stato austriaco, inoltre, ha curato l'implementazione della piattaforma DigLA, ovvero il sistema che consente la conservazione delle memorie digitali che esso custodisce, e si occupa del suo aggiornamento[9].

***Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt* (BMDV)**

A sovrintendere, invece, le questioni relative alla digitalizzazione dell'apparato statale è il Ministero federale per la digitalizzazione e gli affari economici. Questo Ministero ha un raggio di competenze legate all'economia e alla dimensione commerciale, dalla formazione professionale al patrimonio culturale, alle questioni internazionali connesse alla rete dell'Unione europea fino alla digitalizzazione. Riguardo quest'ultima, il dipartimento *Digitalisierung und E-Government* (Digitalizzazione ed E-government) coordina tutte le attività rivolte al digitale e le strutture tecnico-amministrative a questo dedicate. I suoi compiti includono la rappresentanza negli organismi competenti per le ITC e per l'e-government nell'ambito dell'UE e internazionale , nonché la competenza normativa in relazione all'e-government e alla digitalizzazione in Austria. Inoltre, agisce in rappresentanza del proprietario della *Bundesrechenzentrums GmbH* (BRZ), per la predisposizione della strumentazione ITC e delle attività IT del ministero: il BRZ, nello specifico, è il partner tecnologico leader di mercato del settore pubblico in Austria, che utilizza tecnologie come *big data*, intelligenza artificiale e *blockchain* per lo sviluppo dell'amministrazione digitale; in qualità di fornitore di servizi, il BRZ implementa e gestisce soluzioni IT flessibili e automatizzate che soddisfano elevati criteri di sicurezza.

Tra le Agenzie e gli enti coordinati dal BMDW, vanno menzionate, in particolare, le seguenti, in quanto rilevanti per le strategie di digitalizzazione del governo austriaco e, di conseguenza, in qualche modo impattanti sui temi della conservazione digitale.

L'*Angelegenheiten der Digitalisierungsagentur* (Agenzia per la Digitalizzazione - DIA)è il fulcro nazionale per la digitalizzazione: assicura lo sviluppo e il coordinamento della strategia di digitalizzazione nazionale per la trasformazione digitale delle imprese, della società e dell'amministrazione: ha la funzione di supportare l'avvio e la gestione dei progetti con formazione e competenze, avvalendosi dell'azione del Comitato strategico di

[9] Si veda, in proposito, il paragrafo III.2.4.

coordinamento delle politiche digitali, il *Plattform Digitales Österreich* (PDÖ). Questo raggruppa altri due comitati: il primo è il comitato di cooperazione fra Bund, Regioni, Comuni e città metropolitane *Koop-BLSG* (*Bund, Länder, Städte und Gemeinden*), che si compone di quattro gruppi di lavoro permanenti, ovvero Infrastruttura e interoperabilità, Integrazione e accesso, Compliance e sicurezza e Presentazione e Dati standard, che, a loro volta, formano team di progetto specifici. Il secondo è il comitato ICT Federale *IKT-BUND* che, invece, consiglia il ministro del BMDW su questioni generali ICT, nella gestione dei compiti di coordinamento interdipartimentale e predispone l'attuazione di iniziative strategiche, sviluppo e valutazione di progetti, definizione di standard, interfacce e specifiche tecniche.

Inoltre, come nodo strategico dell'e-government in Austria, il PDÖ comprende i *Chief Digital Officers* (CDO) si occupano della pianificazione nel complesso, mentre i *Chief Information Officers* (CPO) si concentrano sulla digitalizzazione dell'amministrazione nel quadro della *Platform Digital Austria*. I membri del gruppo sono i rappresentanti del governo federale, degli stati federali, dell'Associazione dei comuni e delle città, delle imprese, dell'Associazione degli istituti di previdenza sociale austriaci e delle libere professioni: in particolare, l'agenda di quest'organismo è curata dal CIO del governo federale e dal capo del competente dipartimento del BMDW. L'organizzazione, in questo modo è concepita trasversalmente, attraverso la CDO *Taskforce*: in ogni dipartimento è nominato un *Chief Digital Officer* (CDO) per coordinare le questioni di innovazione e digitalizzazione tra i ministeri e per lavorare su una strategia di innovazione e digitalizzazione a livello nazionale. L'ottica adottata è quella di ottimizzare il coordinamento delle misure di digitalizzazione tra i vari dipartimenti: con un approccio uniforme e coerente, questo organismo interdisciplinare austriaco è stato creato dalla BMDW come organo consultivo per le competenze digitali, al fine di produrre raccomandazioni pubblicamente a disposizione e di curare diverse iniziative[10].

L'*Informationsgesellschaft und Beirat für Informationsgesellschaft* (Consiglio consultivo per la società dell'informazione - BIG) è un forum per la cooperazione e lo scambio di

[10] Si menziona, a titolo esemplificativo, DigComp 2.2 AT, su cui si veda il link <https://www.bmdw.gv.at/Themen/Digitalisierung/Gesellschaft/Digitale-Kompetenz_Arbeitsmarkt.html>.

informazioni su questioni legali relative alla digitalizzazione e alla rete tra i ministeri federali, i rappresentanti dell'economia, gli utenti e i fornitori. Nell'ambito del BIG vengono regolarmente organizzate occasioni di scambio di informazioni ed esperienze riguardo a iniziative e misure adottate dai ministeri federali in Austria, nonché nell'ambito dell'Unione europea.

Il *Das Zentrum für sichere Informationstechnologie Austria* (Centro per la tecnologia dell'informazione sicura - Austria - A-SIT), infine, è un'associazione, fondata nel 1999, che assolve le funzioni di centro competente per la sicurezza informatica. Sono membri dell'associazione lo stesso BMDW, la Banca nazionale austriaca, l'Università tecnologica di Graz, il Centro federale di calcolo e l'Università del Danubio di Krems.

III.2.3 Disposizioni sulla conservazione digitale e gli archivi digitali

Il corpus normativo austriaco non include disposizioni specifiche sulla conservazione digitale. Le indicazioni generali si trovano nelle leggi archivistiche emanate tra il 1999 e il 2002: queste, per quanto riguarda la conservazione digitale, vengono 'operativamente integrate' dal progetto DigLA[11].

Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes* e *Gesamte Rechtsvorschrift für Bundesarchivgutverordnung

In linea generale, i riferimenti relativi alla conservazione dei documenti vanno rintracciati nella Legge federale sulla tutela, la conservazione e l'utilizzo dei documenti d'archivio federali (Legge sugli Archivi federali)[12] e nell'Ordinanza del Cancelliere federale sulla classificazione, la trasmissione e la conservazione dei documenti federali (Ordinanza sugli archivi federali)[13]: queste, pur essendo concentrate principalmente sulla dimensione analogica, contengono anche alcuni riferimenti alla documentazione in formato elettronico.

La *Bundesarchivgesetz*, come già menzionato[14], conferisce agli Archivi di Stato austriaci la responsabilità della conservazione della documentazione archivistica delle agenzie

[11] Si veda, in proposito, il paragrafo III.2.4.

[12] *Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes* (*Bundesarchivgesetz*) StF: BGBl. I Nr. 162/1999.

[13] *Verordnung des Bundeskanzlers über die Kennzeichnung, Anbietung und Archivierung von Schriftgut des Bundes* (*Bundesarchivgutverordnung*) StF: BGBl. II Nr. 367/2002.

[14] Si veda il paragrafo III.2.2.

federali, lasciando solo ad alcuni enti la facoltà di mantenere archivi propri[15]: questi, tuttavia, possono consegnare il proprio materiale all'Archivio di Stato austriaco ai fini della tenuta permanente, divenendo proprietà del governo federale[16]. Inoltre, nel caso in cui si debbano conservare immagini, video o audio, il Cancelliere federale può scegliere di ricorrere a strutture specializzate, con cui stabilire un contratto specifico[17].

Riguardo all'eventuale ridistribuzione della documentazione in altri complessi territoriali, il Cancelliere federale è autorizzato, in accordo con il Ministro federale responsabile, a trasferire la proprietà dei documenti d'archivio di competenza dei dipartimenti del governo federale nei *Länder* agli archivi dei rispettivi Stati, nella misura in cui questa documentazione sia principalmente di importanza locale e se la divisione territoriale accetta il trasferimento senza assunzione di onere dei costi da parte dell'Archivio di Stato e assicurando, in ogni caso, i diritti di accesso e di utilizzo[18].

Relativamente alle dinamiche di versamento viene stabilito che il materiale scritto che non contiene dati personali deve essere trasferito entro e non oltre trent'anni dalla conclusione dell'affare in esso trattato (a meno che non vi siano dati che, per legge, determinano un maggior tempo di presso l'ufficio competente).

Nel caso, inoltre, in cui i documenti siano raggruppati in file, questo periodo è determinato dalla data del documento più recente del file. Tale termine temporale costituisce anche il principio del periodo di conservazione presso l'Archivio di Stato. I record contenenti dati personali che dovrebbero essere eliminati in quanto non più necessari allo svolgimento delle pratiche correnti, devono essere sottoposti a valutazione per eventuale valore storico: in caso vi si riscontri, sono consegnati all'Archivio di Stato con in stato di non consultabilità pubblica, con l'indicazione di scadenza di tale periodo di riservatezza[19].

Il governo federale è, dunque, incaricato della selezione e dello scarto: stabilisce con un'ordinanza quali sono i documenti destinati a essere conservato a lungo termine come

[15] § 3 [1,2] *Bundesarchivgesetz BGBl. Nr. 162/1999.* Per l'elenco degli enti autorizzati a tenere il proprio patrimonio documentale, si veda il par. III.2.1 Conservazione digitale e contesto amministrativo.
[16] § 3 [3] *Bundesarchivgesetz BGBl. Nr. 162/1999.*
[17] § 3 [4] *Bundesarchivgesetz BGBl. Nr. 162/1999.*
[18] § 3 [5] *Bundesarchivgesetz BGBl. Nr. 162/1999.*
[19] § 5 [2,3] *Bundesarchivgesetz BGBl. Nr. 162/1999.* Sino al versamento in Archivio di Stato, sono gli enti produttori federali a essere responsabili dei dati personali secondo quanto stabilito nel GDPR.

patrimonio archivistico. Nel caso di documenti su supporto elettronico, l'ordinanza può precisare in quali casi si può prescindere dal già citato obbligo per motivi di realizzabilità tecnica o di motivazioni di natura economica. In linea generale, i materiali analogici devono essere presentati per la presa in consegna in originale, mentre quelli elettronici in una forma che rispetti le regole tecnologiche generalmente riconosciute al momento del versamento. A seguito delle procedure di selezione, sia la documentazione cartacea sia quella digitale vengono eliminate[20].

Gli uffici federali che non hanno la facoltà di gestire autonomamente il proprio archivio devono comunicare all'Archivio di Stato quali documenti conservare con vincolo di riservatezza, su cui poi l'autorità compirà un controllo. Questa, al termine del periodo previsto, determina entro un anno quali documenti sono destinati alla conservazione perenne: a tal fine, l'ufficio versante deve fornire una visione completa dei documenti: se l'Archivio di Stato austriaco non si pronuncia entro questo periodo, i documenti non sono considerati da tenere, in caso di risposta affermativa vengono presi in carico dall'Archivio di Stato austriaco.

Il materiale che proviene direttamente dal Presidente federale, dal Cancelliere federale, dal Vice Cancelliere, da un Ministro federale o Segretario di Stato nell'esercizio delle loro funzioni o nei loro uffici viene trasferito all'Archivio di Stato al termine dell'incarico: questi documenti devono essere tenuti in regime di riservatezza per un periodo di venticinque anni dal momento in cui vengono versati. Salvo diversa disposizione della legge federale, questi documenti possono essere consultati solo con il consenso dell'ex titolare della carica o di una persona da lui designata[21].

La regola generale prevede che dopo trent'anni dal versamento i documenti siano liberamente consultabili, mentre in casi particolari, sulla base della tipologia di dati contenuti, il termine può essere ridotto a vent'anni o esteso a cinquanta[22].

[20] § 5 [4,5] *Bundesarchivgesetz BGBl. Nr. 162/1999*.
[21] § 6 [1-3] *Bundesarchivgesetz BGBl. Nr. 162/1999*.
[22] § 8 [1-6] *Bundesarchivgesetz BGBl. Nr. 162/1999*.

La *Bundesarchivgutverordnung* integra quanto definito nella *Bundesarchivgesetz*, definendo quali documenti sono considerati patrimonio culturale archivistico[23] e come questi debbano essere 'etichettati' per il versamento[24]: stabilisce che vengano trasferiti all'Archivio di Stato quelli non più necessari allo lo svolgimento di affari in corso e se non sono soggetti ad archiviazione particolare secondo le norme sulla sicurezza delle informazioni[25].

Riguardo ai documenti in formato elettronico si specifica che nel caso di sistemi elettronici di archiviazione, si deve garantire che la classificazione e l'ordinamento dei documenti secondo i criteri menzionati per il versamento sia possibile con l'utilizzo di strumenti automatizzati[26]. Inoltre, devono essere versati all'Archivio di Stato in tale forma sulla base dell'interfaccia EDIAKT[27] (nella versione corrente) utilizzando i formati XML per i metadati e PDF per il contenuto.

Vanno comunque conservati in cartaceo i documenti che contengano la firma in originale dei più alti organi di governo, anche se versati come evidenze digitalizzate, se intervengono motivi tecnici che impediscono l'utilizzo dell'interfaccia imposta, sono disponibili in originale solo in cartaceo[28].

In conclusione, si determina che i documenti devono essere scartati, una volta trascorso il necessario periodo di inattività, se il periodo di conservazione previsto dalle ordinanze o

[23] § 2 [1] *Bundesarchivgutverordnung* e *Anlage zu § 2 Abs. 1* (Allegato al § 2 comma 1): per citare alcuni esempi concreti, si tratta di: documenti legislativi (progetti di leggi, ordinanze e trattati statali comprese le dichiarazioni rilasciate su di essi); documentazione relativa allo svolgimento dei compiti costituzionali dell'Assemblea federale, del Consiglio nazionale, del Consiglio federale e dei loro organi, nonché del del Presidente federale e nell'ambito delle attività di controllo della Corte dei conti e dell'Ufficio del difensore civico; Fascicoli personali del presidente federale, del cancelliere federale, del vice cancelliere, dei ministri federali, dei segretari di Stato, dei membri del Consiglio nazionale e del Consiglio federale, del presidente della Corte dei conti, del difensore civico, dei membri della Corte costituzionale, dell'amministrazione Corte, la Corte suprema, i tribunali regionali superiori, la Procura generale e gli uffici del pubblico ministero, il capo di una sezione, gruppo, dipartimento o unità organizzativa analoga nei ministeri federali e altri uffici centrali, nonché i capi delle autorità federali, pubblici ministeri e tribunali, membri del servizio diplomatico superiore e membri delle facoltà universitarie; Materiale scritto proveniente da alti funzionari della pubblica amministrazione (Segretario Generale, Capo Sezione e funzionari comparabili) nell'esercizio della loro funzione; materiale scritto relativo ai rapporti con altri Stati, organizzazioni internazionali, Unione Europea e altri soggetti di diritto internazionale, ecc.

[24] § 3 [1,2] *Bundesarchivgutverordnung*.

[25] § 4 [1] *Bundesarchivgutverordnung.*

[26] § 3 [3] *Bundesarchivgutverordnung.*

[27] Si veda, in proposito, il paragrafo III.2.4.

[28] § 4 [2,3] *Bundesarchivgutverordnung.*

dalle leggi è scaduto, se non sono stati accettati dall'Archivio di Stato per il versamento o se questo non si è pronunciato entro un anno dalla proposta[29].

La conservazione dei documenti fiscali

Nonostante l'assenza di provvedimenti in materia di conservazione digitale, un riscontro concreto delle pratiche in uso (in particolare di ambito privato) può trovarsi nel contesto dell'archiviazione dei documenti fiscali, in particolare delle fatture elettroniche. La normativa in materia, infatti, contempla la conservazione in formato elettronico dei documenti: la *Bundesabgabenordnung* (Legge federale sulle disposizioni generali e sulla procedura per le imposte amministrate dalle autorità fiscali federali, statali e comunali - Codice fiscale federale) stabilisce che i libri contabili ed in generale tutta la documentazione di questa natura possono essere tenuti in modalità informatica; l'obbligo definito è che questi siano leggibili, inalterabili e che ogni modifica possa essere tracciata per tutto il periodo previsto dalla norma[30].

Per tale ragione, la *Wirtschaftskammer Österreich* (WKO – Camera di Commercio austriaca), fornisce al pubblico diverse raccomandazioni in materia di tenuta elettronica delle fatture[31].

La normativa fiscale prevede un periodo di conservazione generale di sette anni per tutti i registri e documenti: le fatture elettroniche, in particolare, danno diritto alla detrazione dell'imposta precedente se l'autenticità dell'origine, l'integrità del contenuto e la leggibilità sono garantite durante il periodo di conservazione.

Per quanto riguarda le fatture in entrata analogiche riprodotte digitalmente, per essere conservate, devono presentare contenuto completo, ordinato e identico all'originale: tali requisiti devono essere garantiti fino alla scadenza del periodo di conservazione previsto dalla legge (il concetto di base è il *revisionssichere Archivierung*, ovvero 'archiviazione a

[29] § 5 [2,3] *Bundesarchivgutverordnung*

[30] § 131 [1] *Bundesgesetz über allgemeine Bestimmungen und das Verfahren für die von den Abgabenbehörden des Bundes, der Länder und Gemeinden verwalteten Abgaben (Bundesabgabenordnung – BAO). StF: BGBl. Nr. 194/1961*.

[31] Si veda, in proposito, la pagina dedicata sul sito istituzionale della *Wirtschaftskammer Österreich* al link <https://www.wko.at/service/innovation-technologie-digitalisierung/elektronische-archivierung-von-rechnungen.html>.

prova di revisione'). Le fatture in uscita emesse utilizzando un sistema IT devono essere in tale forma mantenute nell'originale.

Per poter ottenere tale garanzia, si raccomandano o supporti *write-once read many* (WORM), o software speciali, o fornitori di servizi che offrono la *revisionssichere Archivierung* in modalità cloud.

Oltre al quadro tecnico, si raccomanda la definizione di una procedura uniforme per tutte le fatture, che chi tratta questa tipologia documentale debba essere adeguatamente formato al riguardo e che debba esistere un sistema di controllo interno sul materiale conservato per garantire che solo le persone autorizzate abbiano accesso e che i dati possano essere recuperati in qualsiasi momento.

La stessa WKO raccomanda *e-Tresor*, servizio certificato con l'*Ö-Cloud Gütesiegel*[32].

Questa soluzione, oltre alla possibilità di creare fatture, prevede un modulo 'Archivio', tramite cui conservare i documenti PDF in modo sicuro e immutabile nel centro dell'azienda produttrice A-Trust. I dati vengono conservati nell'archivio WORM, che non consente modifiche successive al contenuto dopo l'archiviazione ed è conforme ai requisiti del BAO, conservando le fatture per sette anni dalla data di acquisizione[33].

III.2.4 Modelli e standard di conservazione

***Digital Long-term Archive* (DigLA)**

Già dal 2004, con l'introduzione dell'*ELAK im Bund* (EiB), l'Austria ha cominciato a far fronte all'introduzione della produzione di documenti in formato elettronico per gli uffici federali: l'ELAK consiste nella strategia e nel progetto di digitalizzazione del governo austriaco, frutto della cooperazione internazionale fra Germania, Austria e Svizzera, che ha come fine quello di fornire una completa gestione degli atti amministrativi, non solo dal punto di vista documentale ma in grado di coprire l'intero procedimento amministrativo sottostante; lo scambio dei documenti si basa sullo standard descrittivo aperto EDIAKT, in formato

[32] Si veda, in proposito, il paragrafo III.2.4.
[33] Su e-Tresor si veda <https://www.e-tresor.at/web/#!infos/archive>.

XML, che rende possibile implementazioni indipendenti e diversi scenari di integrazione[34]. A questa iniziativa fa seguito il riconoscimento della necessità di garantire la conservazione a lungo termine di questo materiale: a partire dal 2006 l'Archivio di Stato austriaco, come organo competente, è stato chiamato a elaborare una strategia e a progettare uno strumento a questo scopo. Nel 2012, a seguito delle fasi di pianificazione, di gare d'appalto e di implementazione, è stato testato il progetto digLA (*Digitale Archiv Osterreich*)[35]. Questo deposito è stato strutturato in conformità con lo standard OAIS, al fine di mantenere la documentazione in esso riposta accessibile, leggibile e riproducibile a lungo termine. I partner tecnologici per la fornitura del software sono Atos IT Solutions and Services e Preservica, mentre il partner contrattuale legale e gestore dell'infrastruttura tecnica è la stessa Cancelleria federale; altri partecipanti al progetto sono il BRZ, come responsabile operativo dell'ELAK e, indirettamente, i fornitori delle relative soluzioni per l'e-Gov.

Inizialmente, l'ingest è stato basato sullo standard EDIAKT II, ma già dal 2013 è stata concepita un'altra interfaccia per accettare modalità indipendenti da EDIAKT II. Per quanto riguarda la conformità agli standard archivistici e tecnici applicabili e ai prodotti software *open source*, sono stati adottati ISDIAH, ISAAR(CPF), ISAD(G) o EAG, EAC-CPF, EAD; METS, PREMIS, PRONOM; DROID, JHOVE[36]. Il PDF/A è il formato preferito: la conversione del contenuto, se tecnicamente possibile, viene effettuata nel corso del processo di *ingest* dal BRZ per conto dei servizi federali che producono i file. Con la *compliance* alla legislazione austriaca in materia di archiviazione e sistemi informatici sono inclusi anche i requisiti di archiviazione ridondante multipla dei dati in luoghi diversi, di sicurezza e protezione dei dati, di *disaster recovery*, di ruoli organizzativi, di definizione dei processi operativi. La sede principale dell'infrastruttura tecnica è a Vienna, la sede secondaria è il

[34] In proposito, si veda la pagina dedicata sul sito web istituzionale del Bundesrechenzentrum Kompetenzzentrum für Digitalisierung (BRZ – Centro Federale di Calcolo - Centro di competenza per la digitalizzazione) al link <https://www.brz.gv.at/was-wir-tun/services-produkte/elak.html>.

[35] Le informazioni sulla piattaforma DigLA sono disponibili sul sito dell'*Österreichisches Staatsarchiv* al link <https://www.oesta.gv.at/ueber-uns/digitales-archiv-oesterreich.html> e tra le risorse Verwaltungs Wiki Österreich <https://www.ag.bka.gv.at/at.gv.bka.wiki-bka/index.php/Hauptseite>. In proposito, si veda anche S. Fröhlich – E. Schöggl-Erns, Digitale Archivierung in Österreich, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 265-274, disponibile online al sito <https://journal.almamater.si/index.php/Atlanti/article/view/134/121>.

[36] Si veda, in proposito, il capitolo I.3.

Centro Alternativo Centrale di Computer del Governo Federale (ZAS) a St. Johann in Pongau.

Per quanto riguarda le procedure amministrative di adesione al progetto, finalizzate a consentire ad altri enti federali di servirsi della soluzione, oltre all'Archivio di Stato, esistono degli appositi comitati digLA: a tale scopo, è sufficiente una semplice dichiarazione di adesione, che comprende opzioni di adattamenti individuali come uno schema di metadati customizzato, una gestione particolare dei ruoli e dei diritti di accesso, mentre ulteriori requisiti specifici possono essere commissionati a spese del richiedente stesso e devono essere concordati separatamente con il partner tecnico. Ogni struttura aderente acquisisce automaticamente una posizione e un voto nei comitati digLA: questi si incontrano regolarmente al fine di ricevere *feedback* e riscontri che costituiscano la base per gli ulteriori sviluppo positivo dell'intero sistema, concordando e prendendo decisioni collettive per le soluzioni ai problemi.

L'archivio digitale *digLA* è stato poi sottoposto a verifiche e valutazioni nel 2018 e aggiornato secondo i più recenti sviluppi tecnologici: l'hardware è stato completamente sostituito nel biennio 2018/2019, mentre dall'inizio del 2020 sono stati ridefiniti l'infrastruttura tecnica e organizzativa, la soluzione software stessa e tutti i processi di conservazione. In particolare, è da segnalare il passaggio, effettuato da maggio 2020, dal formato *ingest* EDIAKT II al formato successivo EDIDOC, che rappresenta il fulcro del Proof of Concept "digLA 2.0", che è stato effettuato da maggio 2020. Il completamento di queste operazioni è atteso entro il 2021, in modo che la conservazione dei dati ELAK accumulati dal 2004 possa successivamente essere eseguita su larga scala.

Tra gli obiettivi futuri di questo progetto, si prevede che l'utilizzo di tutti i materiali archivistici conservati in questo archivio digitale che non sono più soggetti a un regime di accesso limitato sarà reso possibile attraverso una sala di lettura digitale e che la consultazione dei dati sarà supportata dal Sistema Informativo degli Archivi (*Archivinformationssystem* - AIS): questo è già implementato e attivo, ma non ancora a pieno regime, in quanto dalla data di creazione di DigLA non è ancora trascorso un periodo di tempo sufficiente alla libera consultazione dei documenti.

Inoltre, è già stato previsto il flusso in base al quale, eventualmente, per grandi progetti di versamento si debba ricorrere a fornitori esterni di servizi.

Ö-Cloud Gütesiegel

I servizi di conservazione, in Austria, possono essere certificati come servizi cloud.

Affinché le aziende austriache, in particolare le piccole e medie imprese, possano sfruttare le opportunità offerte dal cloud e dai servizi correlati, è stata avviata l'iniziativa *Ö-Cloud Gütesiegel*[37]. La problematica che sta alla base della concezione di tale realizzazione è relativa alla percezione di affidabilità degli utenti nei confronti della qualità dei fornitori dei servizi: dunque, al fine di dare evidenza di garanzia, il BMDW ha promosso questa certificazione: attraverso il suo ottenimento, il prestatore del servizio dimostra la propria aderenza a uno schema di requisiti standardizzato, che riferisce che il soggetto che eroga il servizio risponde a caratteristiche strutturali, infrastrutturali e organizzative di elevata qualità. Questo progetto, inoltre, facilita la cooperazione con altri fornitori di servizi cloud europei e offre ai fornitori nazionali vantaggio competitivo e maggiore attrattiva all'estero.

Il fine del BMDV con Ö-Cloud Initiative, dunque, è promuovere la gestione e l'utilizzo sicuro dei dati attraverso l'adozione di un modello di valutazione condiviso. Infatti, per poter ottenere il sigillo, i fornitori di servizi cloud in Austria seguono diversi step, la cui conclusione con esito positivo, prevedendo anche la pubblicazione dell'esito dell'autovalutazione, assicurano l'impegno del fornitore di rispettare standard di sicurezza internazionali rigorosi e trasparenti e, in particolare, ad attuare il GDPR.

Il primo passo consiste nella registrazione a EuroCloud Austria[38] e nella raccolta del materiale informativo e dei fac-simile della checklist: sono resi disponibili il catalogo

[37] Tutte le informazioni sull'iniziativa Ö-Cloud, così come tutti i documenti necessari ad affrontare la procedura di conseguimento del sigillo, sono consultabili sull'apposito sito web <oe-cloud.gv.at>. Si veda, inoltre, la pagina informativa sulla piattaforma Digital Austria al link <https://www.digitalaustria.gv.at/schwerpunktthemen/Oe_Cloud.html>.

[38] EuroCloud è un'organizzazione indipendente senza scopo di lucro che prevede una configurazione a due livelli, uno generale e uno nazionale, in base a cui ogni Paese europeo può richiedere la partecipazione nel rispetto degli Statuti di EuroCloud (si veda, in proposito <https://eurocloud.org/>); su EuroCloud Austria si veda il sito web istituzionale pubblicato al link <https://www.eurocloud.at/>.

EuroCloud StarAudit, la mappatura dei controlli, le istruzioni per l'utilizzo dello strumento di valutazione e l'Ö-Cloud *stage model*.

Si esegue, poi, l'effettivo *self-assessment* sulla piattaforma StarAudit Assessment Tools, sviluppata nell'ambito dell'iniziativa EuroCloud stessa: questa operazione prevede la compilazione di una griglia che comprende i seguenti settori: *Cloud Service Provider (CSP) Profile*, *Contract*, *Information Security, Operation of Data Center Infrastructure*, *Cloud Service Operational Processes*, *Cloud Service (IaaS - Paas - Saas)*, *Data protection*[39]. I centotrentacinque controlli proposti in queste aree garantiscono all'utente, sia che i dati siano localizzati in Austria sia in Europa, la *compliance* del *provider* a criteri relativi alla trasparenza, alla sicurezza, al funzionamento del data center, ai processi operativi, alle applicazioni come IaaS, PaaS, SaaS, alle condizioni contrattuali, all'organizzazione della protezione dei dati, pianificazione della protezione dei dati, registrazione delle attività di trattamento, modellati sul GDPR, su standard quali ISO 27001 e ISO 20000[40] e sulle raccomandazioni del *Bundesamt für Sicherheit in der Informationstechnik* (BSI - Autorità federale per la sicurezza informatica tedesca)[41].

Dunque, una volta effettuata questa auto-valutazione, il report, scaricabile automaticamente, viene inviato attraverso la piattaforma EuroCloud Austria, e vagliato nell'ambito di EuroCloud Austria stessa: superato questo controllo con esito positivo, si riceva il sigillo di approvazione Ö-Cloud, il quale consente la pubblicazione del servizio per cui si richiede il sigillo nell'elenco pubblico dei prodotti con tale qualificazione[42]. L'inserimento in questa lista è finalizzato alla trasparenza per gli utenti sulle informazioni che i fornitori comunicano, mentre l'aggiornamento costante di queste ultime e la sicurezza del mantenimento dei requisiti viene garantito attraverso la validità annuale del sigillo Ö-Cloud: questo viene considerato valido dal momento in cui il servizio per cui si è avanzata la

[39] Il materiale relativo alle modalità e al contenuto di questo *self-assessment* è disponibile su richiesta, seguendo le istruzioni reperibili al link < https://oe-cloud.eurocloud.at/en/information/>.

[40] Su questi standard si veda il capitolo II.3.

[41] Si veda, in proposito, la pagina dedicata sul sito istituzionale del *Bundesamt für Sicherheit in der Informationstechnik* al link <https://www.bsi.bund.de/EN/Topics/Cyber-Security/Recommendations/Recommendations_node.html>.

[42] La lista dei servizi che presentano tale certificato è consultabile al link <https://oe-cloud.eurocloud.at/veroeffentlichung/>.

richiesta è pubblicato sul sito web oe-cloud.gv.at e sul sito web di EuroCloud e, trascorso un anno, il fornitore deve completare nuovamente la procedura con successo.

Nestor-Siegel für vertrauenswürdige digitale Langzeitarchive

È, infine, da menzionare Nestor, organizzazione attiva su tutto il territorio di lingua tedesca, che si occupa, tra le altre cose, delle certificazioni *ex-post* dei depositi digitali[43]. Questa funzione è svolta per mezzo del *nestor-Siegel für vertrauenswürdige digitale Langzeitarchive* (sigillo Nestor per archivi digitali affidabili): per ottenerlo, è necessario effettuare un processo di autovalutazione sviluppato da Nestor sulla base dello standard DIN 31644:2012-04 *Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive* (Criteri per archivi digitali affidabili)[44].

L'*application* si basa su una checklist di trentaquattro requisiti, che prevedono la descrizione di oggetti informativi e loro rappresentazione, responsabilità per la conservazione, comunità di riferimento, accessibilità, leggibilità, basi legali e contrattuali, conformità normativa, finanziamento, personale, organizzazione e processi, misure di conservazione, gestione di emergenze e migrazioni, caratteristiche significative , integrità (interfaccia di registrazione, funzioni di archiviazione, interfaccia utente), autenticità (registrazione, misure di conservazione, utilizzo), dominio tecnica, SIP, trasformazione dei pacchetti di versamento in pacchetti di archiviazione, pacchetti di archiviazione, leggibilità degli AIP, trasformazione degli AIP in DIP, utilizzo dei pacchetti, identificazione, metadati descrittivi, metadati strutturali, metadati tecnici, *policies* di conservazione a lungo termine, metadati amministrativi, infrastruttura IT e misure di sicurezza.

Il documento risultante viene revisionato nell'ambito di Nestor, che emette un report in cui vengono assegnati punti su ciascun controllo: in caso l'esito comunicato in questa relazione sia positivo, il richiedente è autorizzato a utilizzare ed esporre al pubblico il sigillo Nestor. Questo può essere ottenuto come soluzione indipendente, ma si inserisce anche

[43] Si veda, in proposito, la pagina dedicata sul sito istituzionale Nestor al link <https://www.langzeitarchivierung.de/Webs/nestor/EN/Home/home_node.html>.

[44] Lo standard è disponibile al link <https://www.beuth.de/de/norm/din-31644/147058907> (l'accesso è vincolato al pagamento della risorsa). Il DIN (*Deutsches Institut für Normung*) è l'Istituto tedesco per la standardizzazione: in particolare, si occupa delle norme sulla gestione e conservazione dei documenti il Comitato per l'informazione e la documentazione (*Normenausschuss Information und Dokumentation* - NID).

nell'*European Framework for Audit and Certification*[45]: in aggiunta alla certificazione di base fornita dal *CoreTrustSeal*[46], il sigillo Nestor garantisce un'*Extended Certification*.

[45] Si veda, in proposito, <http://www.trusteddigitalrepository.eu/Welcome.html>.

[46] Si veda, in proposito, il capitolo I.3. Nella scheda informativa citata alla nota 41 si cita il *Data Seal of Approval*, sostituito attualmente dal CTS.

III.3 Francia[1]

III.3.1 Introduzione

La realtà francese mostra una grande sensibilità e un'estrema attenzione al tema degli archivi digitali: la disamina della normativa e degli strumenti sul tema, infatti, evidenzia l'importanza della cultura archivistica nelle scelte intraprese dal governo francese riguardo agli aspetti connessi alla conservazione digitale.

Innanzitutto, è significativa la scelta di affidare agli aggiornamenti conseguenti alla dematerializzazione degli archivi al Codice del Patrimonio Culturale. In questo provvedimento vengono definiti i principi archivistici e illustrate le fasi di evoluzione degli archivi stessi ed è proprio in questo contesto che il legislatore francese ha collocato le disposizioni inerenti alla dimensione digitale, dando vita a un *continuum* analogico-digitale e mantenendo la caratteristica di corpus unitario. Si è mantenuta, infatti, la definizione tradizionale di archivi *courantes*, *intermédiaires* e *définitives*, collocando ciò che riguarda il digitale all'interno di queste stesse fasi e scindendo con precisione le disposizioni relative a ciascuna di esse.

Nella definizione delle modalità attuative di tale normativa, inoltre, si evidenzia l'utilizzo di norme e standard internazionali, affiancati dall'elaborazione di quadri di riferimento nazionali.

A questo *modus operandi* si affianca l'azione di organismi con competenze specifiche sull'ambito della conservazione digitale e della digitalizzazione della Pubblica amministrazione, che collaborano nella definizione di progetti e nell'emanazione di bandi volti a promuoverne la diffusione: questo, al fine di disporre di modelli comuni e minimizzare il ricorso a soggetti terzi per i servizi di archiviazione digitale.

[1] La bibliografia e le risorse telematiche per il contesto francese sono state reperite attraverso i contatti con Martine Sin Blima-Barru, Responsabile del Dipartimento di archiviazione elettronica e degli archivi audiovisuali dell'Archivio Nazionale e col servizio di informazioni al pubblico di quest'ultimo. Si segnalano, inoltre, i riferimenti dei principali siti web istituzionali consultati: *FranceArchives. portail national des archives*, visionabile al link <https://francearchives.fr/fr/>, *Archives Nationales* <https://www.archives-nationales.culture.gouv.fr/fr_FR/web/guest/home> e *Legifrance.Le service public de la diffusion du droit* <https://www.legifrance.gouv.fr/>.

III.3.2 Conservazione digitale e contesto amministrativo: organismi preposti al coordinamento delle politiche sugli archivi

Le questioni inerenti alla gestione e conservazione degli archivi digitali, in Francia, vengono inserite tra le competenze di due principali organismi: il *Service Interministériel des Archives de France* (SIAF - Servizio Interdipartimentale degli Archivi di Francia) e la *Direction interministérielle du numérique et du système d'information et de communication de l'État* (DINUM - Direzione interdipartimentale del sistema di informazione e comunicazione digitale e statale).

***Service Interministériel des Archives de France* (SIAF)**

Il Servizio Interdipartimentale degli Archivi di Francia opera nell'ambito del *Comité interministériel aux Archives de France* (CIAF – Comitato Interministeriale agli Archivi di Francia). Questo, infatti, è uno dei Servizi, insieme a quelli preposti ai musei, al patrimonio e all'architettura, compresi nella *Direction générale des patrimoines* (Direzione generale del patrimonio culturale)[2]. L'organizzazione del SIAF è fissata dall'articolo 3 del decreto del 17 novembre 2009[3], riguardante scopi e organizzazione della Direzione generale del patrimonio culturale. Il SIAF definisce, coordina e valuta le politiche nazionali in materia di versamento, conservazione, comunicazione e valorizzazione di archivi pubblici per scopi amministrativi, civici, scientifici e culturali, ad eccezione di ciò che rientra nelle competenze del Ministero delle Forze Armate e del Ministero per l'Europa e gli Affari Esteri[4]. Ha facoltà decisionale sulle questioni sottoposte dal Direttore degli Archivi di Francia, esercita, in collaborazione con l'Ispettorato generale del patrimonio, il controllo tecnico-scientifico sugli archivi pubblici *courantes* e contribuisce alla salvaguardia degli archivi privati di interesse storico,

[2] Istituita il 13 gennaio 2010 dall'unione delle direzioni dei *musées de France* (DMF), degli *archives de France* (DAF) e dell'*architecture et du patrimoine* (DAPA), la Direzione generale del patrimonio è una delle quattro principali entità del Ministero della Cultura con il *Secrétariat général*, la *Direction générale de la création artistique* e la *Direction générale des médias et des industries culturelles*. Si compone, in base all'art. 1 dell'*Arrêté du 17 novembre 2009 relatif aux missions et à l'organisation de la direction générale des patrimoines,* di *service de l'architecture*, *service interministériel des Archives de France*, *service des musées de France*, *service du patrimoine*, *inspection des patrimoines*, *sous-direction des affaires financières et générales*.

[3] Si veda la nota 2 sull'Arrêté du 17 novembre *2009 relatif aux missions et à l'organisation de la direction générale des patrimoines*.

[4] Secondo l'art. R212-1 del *Code du Patrimoine*, infatti, questi ministeri hanno autonomia nel disporre della documentazione che producono.

nell'ambito delle disposizioni relative alla circolazione dei beni culturali. Si avvale, per queste attività, del supporto del *Conseil Supérieur des Archives* (CSA - Consiglio Superiore per gli Archivi)[5], che viene consultato in materia di archivi pubblici e privati dal Ministro incaricato alla cultura su programmi di ricerca, tematiche legate allo sviluppo di nuove tecnologie nei servizi archivistici e sulla classificazione degli archivi privati come archivi storici.

Questo organismo, dunque, si occupa della supervisione dei tre servizi[6] principali degli Archivi Nazionali di Francia[7] (Archivi Nazionali, *Archives Nationales d'Outre-Mer*, *Archives Nationales du Monde du Travail*), la rete degli archivi in tredici regioni, centouno dipartimenti e diverse città, università e ospedali gestiti dalle autorità locali e lo stesso Servizio Interdipartimentale degli Archivi di Francia. Per questa attività si avvale del sostegno delle *Directions régionales des affaires culturelles* (DRAC).

Il SIAF svolge, in particolare, funzioni fondamentali in relazione agli archivi digitali: non solo si occupa della gestione, dell'amministrazione e del supporto dei sistemi di archiviazione delle amministrazioni centrali dello stato e delle autorità territoriali[8], ma redige ed emette i regolamenti e gli standard di settore.

[5] Viene istituito con il decreto del 21 gennaio 1988 *Arrêté du 21 janvier 1988 portant création du Conseil supérieur des archives*, modificato dai decreti del 17 gennaio 1990 e del 13 settembre 1999.

[6] Vengono così chiamati gli istituti che hanno «*pour missions de collecter, de conserver, d'évaluer, d'organiser, de décrire, de communiquer, de mettre en valeur et de diffuser des archives publiques* » (Art. R212-4-1).

[7] L'Archivio Nazionale di Francia è stato istituito nel 1790, come archivio dell'Assemblea Costituente Nazionale nel corso della Rivoluzione Francese; viene poi riconosciuto, con la legge del 25 giugno 1794, come deposito di tutti gli archivi statali e di tutta la documentazione amministrativa e organizzativa prodotta in epoca monarchica. La stessa legge stabilisce la creazione della rete nazionale degli archivi in ottica centralizzata e il pubblico accesso al patrimonio da essi custodito. Nel 1829 viene creato il Dipartimento degli Archivi, che dal 1936 prende il nome di Direzione degli archivi di Francia, che sovrintende gli archivi dei dipartimenti, delle regioni, dei comuni e degli ospedali, mentre, per quanto riguarda la dipendenza dagli organismi ministeriali, dapprima furono posti tra le competenze del Ministero dell'Interno, poi della Pubblica Istruzione, e, dal 1959, al Ministero della Cultura. Altra tappa fondamentale per il tracciamento di un quadro generale sull'Archivio Nazionale è l'emanazione della legge del 3 gennaio 1979 che, con i decreti annessi, stabilisce le tre età dell'archivio (*courant*, *intermédiair* e *définitif*) e le tempistiche di consultabilità. Attualmente, l'Archivio Nazionale raccoglie, conserva e rende accessibile la documentazione e gli archivi prodotti dal governo e dalle amministrazioni centrali, dai notai di Parigi e da alcuni soggetti privati (Franks, Bernier (a cura di), *The international directory of national archives*, cit., pp. 130-133).

[8] In base all'art. R212-1 del *Code du Patrimoine*, il SIAF esercita tutti i poteri affidati all'amministrazione degli archivi dal codice stesso, ad eccezione di quelli riguardanti gli archivi dei ministeri degli affari esteri e difesa, così come i servizi e le istituzioni che dipendono da essa o sono collegati.

***Direction interministérielle du numérique et du système d'information et de communication de l'État* (DINUM)**

Per quanto riguarda, in proposito, il coordinamento generale delle politiche di digitalizzazione e innovazione tecnologica, che includono anche gli aspetti legati agli archivi digitali e alla loro conservazione, questo è di competenza della Direzione interministeriale del sistema di informazione e comunicazione digitale e statale[9].

È stato costituito con decreto del 25 ottobre 2019[10], attraverso il quale è subentrato alla Direzione interministeriale del digitale e del Sistema di informazione e comunicazione statale (DINSIC) ed è un organismo legato al Primo Ministro posto sotto l'autorità del Ministro dell'Azione e dei Conti Pubblici e messo a disposizione del Ministro dell'Economia e delle Finanze e del Segretario di Stato incaricato per il Digitale. I compiti istituzionali affidati alla DINUM sono l'assistenza ai ministeri e la consulenza al governo per i processi di dematerializzazione e trasformazione digitale, la consulenza al governo e lo sviluppo di servizi e risorse condivise (come la rete interdipartimentale di stato *FranceConnect*, *data.gouv.fr* o *api.gouv.fr*), al fine di migliorare le funzionalità del sistema informativo statale, incrementare la qualità dei servizi pubblici digitali, implementare servizi innovativi per i cittadini. Sta sperimentando, con il supporto dei ministeri, il programma TECH.GOUV per accelerare la trasformazione digitale del servizio pubblico e, nell'ambito del piano *France Relance*, sta supervisionando il passaggio al digitale dello Stato e dei territori per conto del Ministero della Trasformazione e della Funzione pubblica.

III.3.3 Disposizioni sulla conservazione dei documenti e degli archivi digitali

I riferimenti normativi in materia di conservazione digitale si trovano principalmente nel Codice del Patrimonio Culturale, ma vengono integrati con ordinanze, documenti di indirizzo e standard.

Il *Code du Patrimoine* e la conservazione degli archivi digitali

[9] Il sito istituzionale del Direzione interministeriale del sistema di informazione e comunicazione digitale e statale è consultabile al link <https://www.numerique.gouv.fr/>.

[10] *Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numériqueè.*

Il Codice del Patrimonio Culturale[11] contiene tutte le norme relative alla conservazione degli archivi e i vincoli degli enti governativi e le pubbliche amministrazioni per il versamento della propria documentazione agli Archivi Nazionali[12]. Questo prescrive che gli archivi pubblici *courantes* o *intermédiaires* destinati a essere conservati, siano essi analogici o digitali, possono essere gestiti dal competente servizio di archivi pubblici o, previa dichiarazione in merito all'amministrazione archivistica, essere depositati nella totalità o parzialmente presso persone fisiche o giuridiche a tal fine autorizzate dall'amministrazione stessa: questa concessione è oggetto di un contratto, che prevede le condizioni di sicurezza, di accessibilità e di conservazione dei documenti depositati, di controllo di tali documenti da parte dell'amministrazione degli archivi e della restituzione di questi ultimi al depositante alla fine del contratto[13]. A questo proposito sono definiti, di comune accordo tra il servizio, l'istituzione o l'ente interessato e il SIAF, la durata di utilizzo come archivi *courantes* , il periodo di conservazione come archivio *intermédiaire* e la destinazione finale dei documenti al termine del periodo di conservazione negli archivi *intermédiaires* (che sia lo scarto, il trasferimento come archivio definitivo in un servizio di archivi pubblici o il mantenimento nella struttura stessa del servizio, stabilimento o organizzazione interessata)[14].

In particolare, per la conservazione degli archivi digitali, si prevede che possa essere mutualizzata, parzialmente o totalmente, tra più servizi di archivi pubblici e sotto il controllo

[11] *Code du Patrimoine*, approvato con l'*Ordonnance n° 2004-178 du 20 février 2004 relative à la partie législative du code du patrimoine* per la sua parte legislativa, con *Décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres)* e il *Décret n° 2011-574 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine (livres Ier à VI)* per la parte regolamentare.

[12] Il Codice del Patrimonio definisce *archives courantes* gli insiemi di documenti di attuale utilità per l'attività dei servizi, degli enti e delle organizzazioni che li hanno prodotti o ricevuti. La conservazione degli archivi correnti spetta ai soggetti che li hanno prodotti o ricevuti, sotto il controllo del preposto al controllo tecnico-scientifico dello Stato sugli archivi (Art. R212-10). Sono, invece, *archives intermédiaires* quelli che hanno cessato di essere considerati archivi correnti, che non possono ancora, per il loro interesse amministrativo, essere oggetto di selezione ed eliminazione. La loro conservazione può essere assicurata in appositi depositi (di 'prearchiviazione') posti sotto il controllo del responsabile del controllo scientifico e tecnico dello Stato sugli archivi; in alternativa, sono conservati nei locali del servizio, stabilimento o organizzazione di provenienza, su supervisione del responsabile del controllo scientifico e tecnico dello Stato sugli archivi, o in affidamento a soggetti terzi (Art. R212-11). Infine, sono considerati *archives définitives* i depositi di documenti che hanno subito le operazioni di selezione e scarto e che devono essere conservati a tempo indeterminato. La loro conservazione è assicurata nei depositi degli archivi sotto il Servizio interministeriale degli archivi della Francia o posti sotto il controllo del soggetto incaricato del controllo scientifico e tecnico dello Stato sugli archivi.

[13] Art. L212-4, comma II, *Code du Patrimoine*. La responsabilità degli archivi, in ogni caso, resta in capo al soggetto produttore dei documenti, che agisce sotto il controllo dell'amministrazione archivistica.

[14] Art. R212-13 *Code du Patrimoine.*

scientifico dell'amministrazione archivistica: in questo caso, i compiti tecnici e funzionali sono svolti in un sistema di archiviazione elettronica attraverso la condivisione di infrastrutture, personale e risorse materiali, logistiche e finanziarie. La responsabilità dei dati, in ogni caso, rimane in capo al rispettivo servizio di archivio pubblico. Questa circostanza viene delimitata attraverso un accordo, che determina l'ambito d'azione dell''aggregazione', la distribuzione delle funzioni tra le parti e il livello di servizio atteso, le risorse operative, le competenze degli agenti incaricati di svolgere compiti tecnici o funzionali e il quadro finanziario di tale collaborazione[15].

La conservazione condivisa degli archivi digitali risponde a requisiti che riguardano in particolare la sicurezza e la ridondanza delle infrastrutture software e hardware, la gestione del ciclo di vita dei dati e dei relativi metadati, la presenza di meccanismi volti a garantire l'integrità e la leggibilità nel tempo delle informazioni, la tracciabilità di tutte le azioni svolte nel sistema di archiviazione elettronica e la garanzia della restituzione di tutti o parte dei dati, dei loro metadati e delle relative informazioni di tracciabilità[16].

Una volta eseguite le operazioni di selezione e scarto, il Codice del Patrimonio Culturale prevede che gli archivi *définitives* vengano conservati presso la struttura stessa dell'ente produttore o trasferiti al servizio pubblico di archivi competente[17], ma con la stessa possibilità, nel caso degli archivi digitali, di condividere le attività e le strutture di conservazione tra i servizi di archivi pubblici[18]. È stabilito che vengano conservati attraverso

[15] Art. R212-18-1, 2 *Code du Patrimoine*. L'accordo stabilisce anche degli indicatori di monitoraggio, che saranno oggetto di un report redatto su base annuale da ciascun servizio di archivio pubblico responsabile in tutto o in parte del consorzio e inviato a tutti gli attori. Questa relazione viene inviata anche all'organismo preposto al controllo tecnico-scientifico dello Stato sugli archivi (che riceve anche una copia firmata della convenzione), che dispone di un periodo di quattro mesi dal ricevimento della bozza di convenzione per verificarne la rispondenza ai requisiti definiti nell'articolo R. 212-18- 2. In caso di difetto di conformità il contratto non può essere firmato.

[16] Art. R212-18-2 *Code du Patrimoine*.

[17] Art. L212-4, comma I, *Code du Patrimoine*. In base all'art. L212-6, le autorità locali sono proprietarie dei loro archivi e ne garantiscono la conservazione e la valorizzazione; le regioni possono anche affidare la conservazione dei propri archivi, per convenzione, al servizio degli archivi pubblici del dipartimento del capoluogo della regione. L'art. L212-6-1 specifica le condizioni per i gruppi di autorità locali: questi possono affidare la conservazione dei propri archivi, previo accordo, al servizio archivi di uno dei comuni membri del gruppo o depositarli presso il servizio archivi dipartimentale competente (agli artt. L212-11 e L212-12 sono precisate le condizioni per i comuni con più o meno di duemila abitanti).

[18] Art. L212-4-1 *Code du Patrimoine*. Questa disposizione si applica anche si applica alle autorità locali e ai loro gruppi, in deroga ai già citati artt. L. 212-6, L. 212-6-1, L. 212-11 e L. 212-12. I dettagli sulle modalità di condivisione si trovano all'art. R212-18-1.

un servizio pubblico per ragioni legate alla loro natura di beni culturali. Per questa categoria è permesso l'hosting da parte di un provider di terze parti soltanto a condizione che a essere esternalizzata sia soltanto la fornitura del data center (come infrastruttura IT) e che la responsabilità e le operazioni relative a documenti e dati restino interamente a carico del servizio pubblico.

La risposta effettiva per l'applicazione di questi provvedimenti nella pubblica amministrazione è stata fornita attraverso il progetto VITAM: i Ministeri di Forze Armate, Cultura e Affari Esteri, con il coordinamento di CIAF e DINUM, hanno realizzato questa iniziativa al fine di creare la soluzione software gratuita di archiviazione digitale VITAM, che consente la gestione, conservazione e consultazione sicura di volumi molto grandi di archivi digitali *définitives*, *intermédiaires* e *courantes*[19].

Esternalizzazione del servizio di conservazione

Tuttavia, i servizi centrali di pubbliche amministrazioni, gli enti pubblici, le altre persone giuridiche di diritto pubblico e gli organismi di diritto privato responsabili della gestione di un servizio pubblico o di una missione di servizio pubblico possono essere esentati dall'obbligo di versamento a un servizio pubblico, attraverso la sottoscrizione di una convenzione tra l'amministrazione degli archivi e il servizio o l'ente interessato, che stabilisce le condizioni per la gestione, conservazione e accesso al pubblico degli archivi, a condizione che si rispettino i requisiti scientifici e tecnici del SIAF che vi si applicano e che si impieghi un incaricato qualificato dell'archivio[20].

Riguardo a questa possibilità di esternalizzare i servizi di archiviazione, il quadro di riferimento parte ancora una volta dal Codice del Patrimonio, che è stato recentemente integrato dal Decreto 2020-733 del 15 giugno 2020 relativo al decentramento delle singole decisioni amministrative in campo culturale[21]; questo ha apportato delle semplificazioni alla procedura di rilascio dell'autorizzazione a partire dal gennaio 2021. Per gli archivi *courantes* e *intermédiaires* il ricorso a un prestatore di servizi deve essere formalizzato attraverso un

[19] Per la trattazione approfondita di questo progetto, si veda il paragrafo III.3.4.
[20] Art. R212-12 *Code du Patrimoine.*
[21] Décret n° 2020-733 du 15 juin 2020 *relatif à la déconcentration des décisions administratives individuelles dans le domaine de la culture*.

contratto[22] e indicato nella dichiarazione di deposito degli archivi *courantes* o *intermédiaires*[23] che, insieme alle informazioni relative al contesto, agli obiettivi, al programma e alla durata stimata dell'operazione e ai dettagli sul materiale versato e ai servizi[24], deve contenere informazioni sulle condizioni per il ricorso a fornitori di servizi esterni e sugli impegni del depositario affinché tale ricorso fornisca un livello equivalente di garanzia rispetto agli obblighi gravanti sull'attività di custodia. È previsto, per quanto concerne i requisiti generali, che qualsiasi persona fisica o giuridica voglia beneficiare dell'autorizzazione di svolgere attività di outsourcing debba possedere la certificazione corrispondente agli standard relativi all'archiviazione elettronica, secondo le norme di riferimento stabilite con ordinanza del Ministro responsabile della cultura[25] e individuare i responsabili dell'attività di conservazione, specificando il legame contrattuale tra loro e il depositario[26]. Nello specifico, l'Ordinanza del 4 dicembre 2009 del Ministro della Cultura riguardante le norme in materia di archiviazione e servizi di gestione in outsourcing prescrive che il riferimento per questi ultimi è lo standard NF Z 42-013[27], con la raccomandazione di conformarsi a ISO 14721[28].

Per quanto riguarda processo di rilascio dell'autorizzazione a fornire servizi di archiviazione in outsourcing, l'obbligo di inoltro di una domanda al SIAF[29] e il successivo

[22] Art. L212-4 *Code du Patrimoine.* Il deposito è oggetto di un contratto che prevede le condizioni di sicurezza e conservazione dei documenti depositati nonché i termini di accesso, il controllo di tali documenti da parte dell'amministrazione degli archivi e la loro restituzione al depositante alla fine del contratto. Questo contratto, di cui il preposto al controllo tecnico-scientifico dello Stato sugli archivi riceve copia firmata (Art. R212-21), contiene clausole relative a: natura e supporto degli archivi depositati; descrizione dei servizi forniti; descrizione dei mezzi per la prestazione dei servizi; dispositivi per la comunicazione materiale e l'accesso agli archivi da parte del depositante; obblighi verso il depositante in caso di modifiche o sviluppi tecnici; informazioni sulle garanzie che consentono di coprire eventuali inadempienze del depositario; disposizioni per il ripristino degli archivi depositati al termine del contratto di deposito, unitamente all'impegno alla completa distruzione delle copie che il depositario ha effettuato durante la durata del contratto; polizze assicurative che il depositario stipula a copertura dei danni e delle perdite che dovessero subire gli archivi depositati; la durata del contratto e le condizioni di eventuale rinnovo (Artt. R212- 22, *Code du Patrimoine*).

[23] Artt. R212-19 e 20, *Code du Patrimoine*. La dichiarazione di deposito degli archivi correnti e intermedi di cui al comma II dell'articolo L. 212-4 è inviata, mediante lettera raccomandata con avviso di ricevimento, al Responsabile del controllo tecnico-scientifico dello Stato sugli archivi.

[24] Artt. R212-20 e 22, *Code du Patrimoine*.

[25] Si veda l'Arrêté du 4 décembre 2009 *précisant les normes relatives aux prestations en archivage et gestion externalisée*.

[26] Art. R212-23, *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733.

[27] Si veda il paragrafo III.3.4.

[28] Arrêté du 4 décembre 2009 *précisant les normes relatives aux prestations en archivage et gestion externalisée*.

[29] L'art. R212-25, *Code du patrimoine,* prima dell'entrata in vigore del Decreto n.2020-733, identificava come mandatoria la presentazione di una domanda di autorizzazione al SIAF, che doveva contenere

iter istruttorio da esso condotto stabiliti precedentemente nel *Code du Patrimoine* sono stati sostituiti dall'audit di certificazione per lo standard NF 461 prima del rilascio del benestare da parte del prefetto, al quale deve essere inviata la richiesta di questa autorizzazione in luogo del SIAF. Queste modifiche sono state effettuate nell'ottica di decentralizzare le decisioni amministrative nel campo della cultura e del patrimonio e gestirle a livello territoriale. Dunque, le visite di auditor di certificazione dell'organismo AFNOR, emittente degli standard[30], prendono il posto delle visite preventive in loco effettuate dal SIAF per la concessione dell'accreditamento o per rinnovi. Inoltre, non vi è più il vincolo di invio della bozza di contratto di esternalizzazione al responsabile del controllo tecnico-scientifico prima della sottoscrizione.

È importante menzionare anche l'abolizione dell'obbligo, precedentemente in vigore, di localizzazione sul territorio nazionale degli archivi *courantes* e *intermédiaires*[31], incompatibile di diritto con la normativa europea in materia di libera circolazione dei dati[32].

Restano, comunque, la legittimità dei direttori degli archivi dipartimentali ad intervenire nell'ambito del controllo tecnico-scientifico dello Stato sugli archivi[33], in particolare per eventuali visite in loco di ispezione sui documenti da esternalizzare o esternalizzati, il supporto agli archivisti con i fornitori, in particolare sui termini dei contratti o sulla rilevanza dell'archiviazione esterna o interna, in Francia o all'estero, in base alla rilevanza degli

informazioni complete e dettagliate circa il soggetto richiedente, le sue qualifiche e i requisiti sopra menzionati. L'art. R212- 27 specificava ulteriori indicazioni aggiuntive sulla località di collocazione delle infrastrutture, la descrizione degli strumenti hardware e software e delle loro funzionalità e dettagli sulle misure di sicurezza e di mantenimento dell'integrità del contenuto.

[30] L'associazione AFNOR e le sue filiali costituiscono un gruppo internazionale al servizio dell'interesse generale e dello sviluppo economico, che si occupa di progettare soluzioni basate su standard. Il supporto di questa associazione avviene attraverso quattro aree di competenza; la prima è quella di *normalisation*: AFNOR Standardization supporta il sistema di standardizzazione francese nell'elaborazione di norme nazionali e internazionali; la seconda è l'area *édition*: AFNOR distribuisce standard facoltativi in Francia, garantendone la revisione e l'aggiornamento; AFNOR *compétences* offre corsi di formazione alle organizzazioni e alle figure professionali al fine di fornire competenze sul contesto normativo e tecnico; infine, AFNOR *certification* fornisce prestazioni per la certificazione e valutazione di prodotti, sistemi, servizi e competenze, rilasciati con marchi quali AFAQ, NF o il marchio europeo di qualità ecologica (<https://www.afnor.org/> - ultima consultazione 01/02/2021).

[31]Comma II art. R212-23 *Code du patrimoine,* abrogato dal Decreto n. 2020-733.

[32] Reg. EU 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[33] Art. R212-19 a R212-22 *Code du Patrimoine.*

archivi. La SIAF continuerà ad aggiornare la pagina sul portale *FranceArchives*[34] sui regolamenti, i termini e le condizioni di approvazione, compreso l'elenco aggiornato dei fornitori di servizi approvati.

La nuova procedura, dunque, si avvale della convergenza dei criteri di qualità AFNOR con quelli previsti dal Decreto del 4 dicembre 2009. Innanzitutto, la società che eroga servizi di archiviazione in esternalizzazione richiede l'approvazione (o il rinnovo dell'approvazione) per uno o più siti certificati NF 461. La richiesta è rivolta al prefetto del dipartimento in cui ha sede la società, o al *préfet de police* per le società internazionali che non hanno una filiale con sede legale in Francia[35]. La richiesta viene poi trasmessa al direttore degli archivi dipartimentali interessati, il quale verifica l'esistenza di un certificato valido per uso commerciale e propone al prefetto un provvedimento che consenta alla società di custodire archivi pubblici *courantes* e *intermédiaires* nei siti menzionati nel certificato. Una volta ottenuta l'autorizzazione a prestare servizi di archiviazione in esternalizzazione[36], questa ha la stessa durata della relativa certificazione attestante il rispetto delle norme, con possibilità di rinnovo[37]. L'azienda può effettuare il rinnovo[38] finché desideri continuare la sua attività di conservazione, il quale viene concesso in caso gli audit di certificazione non rivelino delle

[34] Il portale *FranceArchives* è accessibile al link <https://francearchives.fr/fr/>. Questo portale, inoltre, riunisce in un'unica struttura, tutti i siti web degli archivi territoriali, utilizzando il web semantico.

[35] L'art. R. 212-25 *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733, stabilisce che il richiedente il benestare deve rivolgersi al prefetto del dipartimento in cui si trova la sede della sua società o della sua filiale controllata o al prefetto di polizia per le società estere non aventi sede legale in Francia, mediante lettera raccomandata con ricevuta di ritorno, inviando un dossier contenente l'identità e l'indirizzo del richiedente o del suo rappresentante nonché, per le persone giuridiche, lo status; i documenti relativi alle certificazioni, attestanti la loro validità e la conformità alle norme di cui all'articolo R. 212-23 o l'indirizzo delle pagine Internet di riferimento che attestino l'attuale validità di tali certificazioni.

[36] Art. R212-28, *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733: il prefetto emette la propria decisione entro quattro mesi dalla richiesta di approvazione, di cui è notificata la ricezione. Durante questo periodo, il prefetto può eseguire, da solo o attraverso qualsiasi persona delegata a tal fine, un controllo documentario e in loco degli elementi forniti dal richiedente. Un non riscontro per quattro mesi costituisce una decisione implicita di rigetto. L'elenco dei fornitori di servizi di conservazione autorizzati (attualmente in numero di 18) è pubblicato e curato dal SIAF sul proprio sito istituzionale (è consultabile al link <https://francearchives.fr/fr/article/26287437>).

[37] Art. R212-29, *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733: L'autorizzazione di cui all'articolo R. 212-23 è rilasciata per la durata della relativa certificazione attestante il rispetto delle norme di cui all'articolo R. 212-23, ed automaticamente prorogata in caso di rinnovo. La persona abilitata informa immediatamente il prefetto che ha concesso il benestare di ogni modifica che riguardi le informazioni di cui all'articolo R. 212-25 e di ogni interruzione, temporanea o permanente, della sua attività.

[38] Un'azienda può richiedere, durante un rinnovo di certificazione, anche l'aggiunta di un nuovo sito o edificio: in questo caso, verrà inviata una nuova richiesta al prefetto competente per l'approvazione.

non conformità; in tal caso, ne viene richiesta la risoluzione, pena la non estensione della validità del certificato[39].

La conservazione dei dati sanitari: un caso specifico

È da segnalare, infine, il caso dei dati sanitari personali, in quanto il processo di autorizzazione per l'hosting di documenti contenenti tali informazioni è oggetto di provvedimenti specifici indicati dal SIAF sul proprio sito istituzionale, insieme alle indicazioni generali sulla conservazione digitale. Infatti, anche i dati raccolti durante attività di prevenzione, diagnosi, cura o monitoraggio sociale e medico-sociale che non sono stati ancora oggetto di selezione possono essere affidati, previa dichiarazione all'amministrazione degli archivi, a persone fisiche o giuridiche titolari della certificazione NF461[40]. I fornitori di sistemi informatici sanitari che erogano dei servizi agli ospedali, cliniche, case di cura ecc. devono, per conservare i dati sanitari sui loro server, di essere accreditati quali conformi alla norma 27001; inoltre, gli se gli stessi fornitori offrono delle prestazioni di conservazione digitale, devono adeguarsi alle disposizioni inerenti agli archivi già segnalate: prima del 2021

[39] Art. R. 212-31, *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733: il ritiro per qualunque motivo di una certificazione attestante la conformità alle norme di cui all'articolo R. 212-23 comporta automaticamente la revoca dell'autorizzazione. In caso di scadenza di tale certificazione, l'autorizzazione può essere sospesa solo se è in corso il rinnovo della certificazione e sottoposto all'autorità di certificazione. In attesa di una decisione definitiva sul rinnovo, è consentita la conservazione degli archivi già depositati, ma l'approvazione risulta sospesa per l'acquisizione di nuovi archivi. In caso di divulgazione non autorizzata o di gravi violazioni da parte del depositario, in particolare se riguardano la compromissione di riservatezza, l'integrità, sicurezza e la longevità degli archivi depositati, il prefetto che ha concesso il benestare può, a titolo cautelativo, in attesa di una decisione definitiva sulla revoca dell'autorizzazione, sospendere l'autorizzazione di acquisizione di nuovi depositi. Nel valutare la revoca, il Prefetto comunica le ragioni alla persona autorizzata, mediante lettera raccomandata con avviso di ricevimento, e chiede che le sue osservazioni siano formulate entro due mesi, per iscritto o, su sua richiesta, oralmente, con la possibilità di assistenza e rappresentanza di un avvocato. La decisione di revocare il consenso viene notificata all'interessato autorizzato, mediante lettera raccomandata con avviso di ricevimento, è motivato e menziona i mezzi e i termini per l'appello. Termina automaticamente la conservazione degli archivi depositati e ne comporta la restituzione ai depositanti. I costi di ripristino degli archivi depositati sono a carico del depositario. Le decisioni di revocare l'approvazione sono pubblicate nella raccolta degli atti amministrativi della prefettura.

[40] In base all'art. R1111-16 del *Code de la santé publique* i prestatori di servizi abilitati dal Ministro della Cultura per la conservazione degli archivi pubblici correnti e intermedi su carta, possono erogare l'hosting di dati sanitari personali su supporto cartaceo e degli archivi pubblici o privati che contengono tali dati sanitari personali. Precedentemente, questa circostanza richiedeva anche un'autorizzazione, rilasciata dal Ministro della salute (artt. L.1111-8, R.1111-9-R.1111-15-1 *Code de la santé publique*), sia per archivi pubblici sia privati. Tale situazione è stata modificata dall'Ordonnance n° 2017-27 du 12 janvier 2017 *relative à l'hébergement de données de santé à caractère personnel*, che ha determinato che i prestatori di servizi autorizzati dal Ministro della Cultura per la conservazione degli archivi pubblici correnti e intermedi su supporto cartaceo o digitale hanno la facoltà di offrire un servizio di conservazione in outsourcing dei dati sanitari personali su supporto cartaceo o digitale (siano essi depositati in archivi di strutture pubbliche o private).

la candidatura era valutata dal Ministero della cultura con un esame delle misure di protezione dai rischi più celebre rispetto alla conformità a ISO 27001; dal primo gennaio 2021 è necessario l'accreditamento NF 461 e la procedura è semplificata, in quanto il nuovo regolamento pubblicato prevede una riduzione di una giornata del tempo di audit necessario, dato che il richiedente è già conforme a ISO 27001.

III.3.4 Modelli e standard di conservazione

***Valeurs Immatérielles Transmises aux Archives pour Mémoire* (VITAM)**

Il modello di conservazione implementato dal governo francese è inquadrato dal già citato progetto VITAM, *Valeurs Immatérielles Transmises aux Archives pour Mémoire*[41], che ha come obiettivo l'implementazione di una suite scalabile e interoperabile per la conservazione digitale. I ministeri degli Affari Esteri e Sviluppo Internazionale, della Cultura e della Difesa, hanno intrapreso questo piano d'azione per rispondere congiuntamente alla sfida dell'archiviazione digitale, in tutte le sue fasi: l'iniziativa è stata convalidata dal CIAF e sostenuta dalla DINUM nel 2013 e oggetto di un accordo tra i tre ministeri e i servizi del Presidente del Consiglio nel 2015, anno a cui risale l'avvio col coordinamento degli stessi CIAF e DINUM.

Gli obiettivi del progetto sono la creazione della soluzione software gratuita di archiviazione digitale VITAM che consente la gestione, la conservazione e la consultazione in sicurezza di archivi *courantes*, *intermédiaires* e *définitives*; l'implementazione di piattaforme di archiviazione che utilizzino la soluzione VITAM in ciascuno dei tre ministeri ideatori, tramite i progetti SAPHIR per il Ministero degli Esteri, ADAMANT per il Ministero dei Beni Culturali e gli Archivi Nazionali e ARCHIPEL per il Ministero della Difesa[42];

[41] Il progetto VITAM è inquadrato come parte dell'azione "*Transition numérique de l'État et modernisation de l'action publique"* del Programma Investimenti per il Futuro (*Programme d'investissements d'avenir*- PIA). Il manifesto Agile del progetto dichiara che la soluzione VITAM è concepita per i servizi di amministrazione, al fine di affrontare le sfide dell'accesso nel tempo alle proprie informazioni digitali; essa offre una soluzione software gratuita per l'archiviazione, scalabile, semplice e facilmente interfacciabile, che consente la gestione unitaria e sicura di miliardi di oggetti e mira alla sua adozione da parte del maggior numero di attori pubblici.

Nel sito istituzionale di VITAM, consultabile al link <https://www.programmevitam.fr/>, sono illustrate tutte le informazioni inerenti al progetto e sono resi disponibili tanto la documentazione tecnica e operativa quanto gli strumenti per gli sviluppatori.

[42] Si vedano, rispettivamente, per SAPHIR <https://www.programmevitam.fr/ressources/RefCourant/20201002_Vitamenligne_Saphir2.pdf>, per ADAMANT <https://www.culture.gouv.fr/Presse/Communiques-de-presse/ADAMANT-Lancement-le-7-

infine, la più ampia distribuzione e riutilizzo del software: è prevista la garanzia del sostegno finanziario e il supporto nella fase di implementazione, attraverso i progetti correlati ANET (*Archivage numérique en Territoires*)[43] per gli enti locali e DiAMAN (*Dispositif d'Accompagnement des Missions pour l'Archivage Numérique*)[44] nell'ambito del Ministero della Cultura e del SIAF, e i relativi bandi di gara. Queste iniziative risultano ampiamente accolte ed efficaci[45]: i dati rilevati nel report di bilancio delle sei edizioni di *call for projects* AD-ESSOR[46], predecessore del progetto ANET per il quinquennio 2014-2019, mostrano che nel 2014 il 39% dei comuni ha dichiarato di aver svolto azioni a favore dell'archiviazione elettronica, mentre nel 2018 questa cifra è salita al 71%; nei dipartimenti la tendenza è ancora più evidente: il dislivello marca sei dipartimenti con sistemi di archiviazione elettronica su

decembre-d-une-nouvelle-plateforme-d-archivage-numerique-pour-les-Archives-nationales> e per ARCHIPEL <https://www.servicehistorique.sga.defense.gouv.fr/actualites/ouverture-de-service-darchipel-le-systeme-darchivage-hybride-du-ministere-des-armees>.

[43] Al termine del progetto AD-Essor (2014-2019), che ha consentito il supporto di 141 progetti in cinque anni, il SIAF ha realizzato l'iniziativa ANET, per continuare a sostenere i servizi nello sviluppo dei propri sistemi di archiviazione digitale, che: la complessità dell'implementazione di tali sistemi richiede sforzi pluriennali e comporta la definizione di una strategia, la scelta di un'organizzazione, l'integrazione del quadro normativo e azioni concrete a sostegno dei servizi (a proposito, si veda <https://francearchives.fr/fr/article/171593987>).

[44] Dal 2014, con DiAMAN, il SIAF supporta lo sviluppo di soluzioni per gli archivi digitali *intermédiaires* e *définitives*. DiAMAN mira a promuovere l'attuazione delle politiche di archiviazione digitale globale nei dipartimenti ministeriali: ogni intervento è concepito in modo tale da portare a deliverable immediatamente fruibili dai soggetti interessati per i sistemi informativi ministeriali, in modo tale da fungere da 'esperimento' applicabile ad altri dipartimenti ed enti e riutilizzato nel contesto del programma VITAM (a proposito, si veda <https://francearchives.fr/fr/article/97846804> - ultima consultazione 03/02/2021).

[45] È da sottolineare che è prevista, per principio, una significativa partecipazione attiva della comunità di riferimento: si basa, secondo il profilo Agile, su una forte interazione con gli utenti attraverso la partecipazione a *workshop* e *feedback* sui casi d'uso. I workshop, organizzati con archivisti di vari enti pubblici, hanno avuto luogo dal 2015 e si svolgono correntemente con due obiettivi primari: predisporre gli aspetti funzionali per lo sviluppo, attraverso la comprensione delle esigenze generali e promuovere la condivisione delle riflessioni dei progetti ministeriali e dei partner sulla necessità di adattare il software (front office) del proprio servizio archivi. I lavori svolti tra 2015 e 2017 sono stati incentrati sulla preparazione dei depositi di archivi digitali, sulle modalità di versamento, conservazione, ricerca e accesso. Dal 2017, parallelamente all'avanzamento del lavoro di progettazione, si è intensificato l'approfondimento di temi quali estrazione ed elaborazione di documenti (migrazione dei formati, generazione automatica di metadati, anonimizzazione, ecc.), garanzia del valore probatorio dei documenti conservati, gestione degli archivi classificati e conservazione a lungo termine. La collaborazione è basata su quattro livelli di partnership, oggetto di accordi: il primo prevede la partecipazione alla riflessione tecnica e funzionale, con sperimentazioni su esportazione di dati, installazione e utilizzo di strumenti identificati e sondaggi, il secondo il contributo allo sviluppo effettivo della soluzione VITAM, con l'esecuzione di test funzionali e tecnici al termine dei principali cicli di consegna, il terzo l'implementazione del software con strumenti già a disposizione e l'ultimo il restituire gli esiti alla comunità.

[46] Il documento *Appel à projets AD-ESSOR 2014-2019 – Bilan*, rilasciato il 10 settembre 2019, è consultabile al link <https://francearchives.fr/file/3e4df0413e1f2f7d8aec0112be49c962c058b837/20190906_Bilan_AAP_AD-Essor_vdiffusion.pdf>.

101 nel 2014, 35 dipartimenti nel 2018, di cui 26 beneficiari di una sovvenzione AD-ESSOR dal 2014.

Dal punto di vista tecnico, si è scelto di realizzare un software liberamente utilizzabile[47], che consente una spiccata interoperabilità: è pensata per essere interfacciata con le applicazioni già esistenti presso i soggetti produttori e i loro software di gestione degli archivi. Lo strumento VITAM fornisce supporto per diversi tipi di oggetti digitali: tra i più significativi vi sono documenti, immagini statiche e dinamiche, registrazioni audio, messaggi elettronici e messaggistica.

L'obbligo di implementare una soluzione di archiviazione digitale nei contesti dei tre ministeri promotori, molto diversi in termini di pratiche archivistiche e di produzione informatica, ha determinato la scelta di realizzare un back office, secondo la logica di un *minimum viable product*: l'obiettivo è includere nel software il numero massimo di funzioni mutuabili e tecnologicamente complesse, ma di lasciare a ciascuna entità la possibilità di implementare strumenti adatti alle proprie specificità. Dunque, VITAM si inquadra come 'mattone infrastrutturale', volto ad assicurare la conservazione a lungo termine dei documenti digitali presentati e a garantirne il mantenimento del valore probatorio: l'uso condiviso tra più organizzazioni ha guidato verso un'impostazione *multi-tenant*, con separazione sistematica per organizzazione-utente di tutti gli archivi e le informazioni del sistema. Le API forniscono, principalmente, funzionalità di versamento dei documenti, gestione e indicizzazione dei metadati, gestione sicura dell'infrastruttura di archiviazione, trasformazione dei file, accesso, ricerca e consultazione.

Più specificamente, l'architettura del sistema è tecnologicamente il più neutra possibile: non impone alcuna infrastruttura o strumento particolari, si installa su un ambiente server fisico x86, virtualizzato o in cloud, in base alle scelte dell'organismo che lo adotta, con più o meno automazione; è sviluppato per funzionare su un ambiente Linux e distribuito per una distribuzione CentOS (e anche in Debian in V1); fornisce una soluzione di storage implementabile su qualsiasi infrastruttura server in relaziona alla capacità di archiviazione

[47] È sviluppato principalmente in Java, il codice è concesso sotto licenza CeCILL V2.1 (si veda, in proposito, <https://cecill.info/licences.en.html>), compatibile GNU General Public License (si veda, in proposito, <https://www.gnu.org/licenses/gpl-3.0.html>), e la documentazione è disponibile con Open License V2.0 (<https://www.etalab.gouv.fr/wp-content/uploads/2017/04/ETALAB-Licence-Ouverte-v2.0.pdf>).

del disco o può utilizzare strumenti esistenti di archiviazione Object (Swift), se presenti. Una piattaforma di archiviazione che utilizza il software VITAM include applicazioni di front office, che consentono agli utenti di accedere agli oggetti archiviati a scopo di ricerca, consultazione, gestione o conservazione, che a loro volta comprendono il front-end archivistico (IHM, Archival Information System) e le applicazioni di terzi di cui il soggetto produttore si avvale; si compone, inoltre, di un back office che si appoggia su offerte di archiviazione, alcune delle quali potenzialmente di terze parti, che garantiscono la conservazione binaria degli oggetti archiviati e di applicazioni di terze parti, che caricano e visualizzano oggetti nella piattaforma.

Il codice fornito in licenza gratuita consente di implementare questo nucleo di VITAM, il back office vero e proprio: comprende API di tipo REST e JSON, incluse quelle per la sua amministrazione, in quanto deve essere completamente integrabile e qualsiasi funzione deve poter essere mobilitata, tramite API, da un front-end non VITAM, IHM (*Interface Homme-machine*) di amministrazione standard e dimostrative e un'opzione di archiviazione (è possibile utilizzare offerte di *object storage* esterno, oppure implementarle attraverso il software VITAM)[48].

È, infine, conforme alle norme e agli standard SEDA e NF Z42-013[49] e si basa sul modello OAIS, di cui presenta le aree funzionali; a queste è stata aggiunta una specifica area funzionale denominata "*gestion des archives existantes*" (gestione degli archivi esistenti), che riunisce le attività di aggiunta e modifica dei metadati, eliminazione, regole di gestione[50], trasferimento ad altro *Sistème d'Archivage Eléctronique* (SAE): questa include interfacce applicative aggiuntive per scopi più specificatamente di gestione corrente e amministrazione.

NF Z42-013 e NF 461

[48] Le componenti di VITAM e gli strumenti per gli sviluppatori sono dettagliate nella sezione Documentation del sito istituzionale, consultabile al link <https://www.programmevitam.fr/pages/documentation/>)

[49] Si veda *infra.*

[50] Ci si riferisce alle *Règles de gestion et de sélection des archives*, linee guida emanate dal SIAF in adempimento alle operazioni di gestione, selezione e scarto menzionate agli artt. L212-2 e 3 e R212-14 *Code du Patrimoine*. Si sottolinea che qualsiasi amministrazione deve, in particolare, concordare con l'amministrazione degli Archives de France la durata dell'utilità amministrativa (*Durées d'Utilité Administrative* - DUA) dei documenti e dei dati che produce, nonché predisporre la loro conservazione finale o eliminazione.

Nel caso in cui un ente pubblico non aderisca a questo programma, ma scelga di usufruire di un servizio di conservazione in esternalizzazione, deve affidarsi a soggetti autorizzati, che, come si è detto, devono essere conformi a standard e schemi entro cui implementare i sistemi di archiviazione, che stabiliscono anche dei vincoli sulla sicurezza e sull'interoperabilità, tra cui i già citati NF Z42-013 e SEDA.

Lo standard NF Z42-013 *Archivage électronique - Recommandations et exigences*[51], menzionato dal Decreto del 4 dicembre 2009, descrive le misure tecniche per la progettazione e al funzionamento dei sistemi informatici al fine di garantire la conservazione e l'integrità dei documenti in essi archiviati[52], i processi organizzativi da attuare per l'archiviazione dei documenti elettronici e l'impostazione dell'offerta di servizi proposta ai clienti esterni o interni del servizio di archiviazione: si tratta più di uno standard tecnico che di uno standard funzionale, in quanto si concentra in particolare sulla tracciabilità dei processi implementati per l'archiviazione elettronica e sui requisiti di sistema in termini di sicurezza e accesso; definisce, inoltre, le clausole necessarie in un contratto di servizio concluso con un conservatore di terze parti.

[51] A proposito, si veda <https://francearchives.fr/fr/article/91524937>.

[52] Riguardo all'integrità dei documenti, è necessario menzionare lo standard NF Z42-026 *Définition et spécifications des prestations de numérisation fidèle de documents et contrôle de ces prestations* (Definizione e specifiche dei servizi per la digitalizzazione fedele dei documenti cartacei e il controllo di questi servizi). La dematerializzazione di documenti e processi dell'amministrazione ha posto, anche in Francia, la questione del trasferimento del valore probatorio dell'atto scritto su supporto cartaceo alla sua copia su supporto informatico e, una volta effettuata la trasposizione, sulla possibilità di eliminare l'originale. L'Ordonnance n° 2016-131 du 10 février 2016 *portant réforme du droit des contrats, du régime général et de la preuve des obligations* che ha modificato l'articolo 1379 del Codice civile francese, stabilisce che una copia elettronica ritenuta affidabile ha la stessa forza probatoria dell'originale; la natura affidabile della copia è valutata a discrezione del giudice, ma si si presume tale se sono soddisfatte determinate condizioni di riproduzione (riproduzione identica della forma e del contenuto dell'atto) e conservazione (integrità garantita nel tempo). Il Décret n° 2016-1673 du 5 décembre 2016 *relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil* chiarisce le condizioni affinché una copia possa beneficiare di una presunzione di affidabilità. Nel 2014 è stato emesso dagli Archivi di Francia uno strumento decisionale e metodologico, il vademecum *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision?* (consultabile al link <https://francearchives.fr/file/f3e02b58b9f9ef87725ecf422da10422270852e0/static_7429.pdf>) destinato ai preposti al controllo tecnico-scientifico degli archivi pubblici, al fine di valutare i progetti di dematerializzazione e i rischi dell'eliminazione degli originali. Questo, dal 2017, si basa sullo standard AFNOR NF Z42-026 *Définition et spécifications des prestations de numérisation fidèle de documents et contrôle de ces prestations*: in esso vengono determinate le responsabilità dei vari attori della digitalizzazione e definite le misure che contribuiscono alla realizzazione di una digitalizzazione "fedele"; questa norma è stata elaborata in integrazione allo standard NF Z42-013: questo, infatti, permette di definire, una volta effettuata la digitalizzazione, le condizioni di conservazione della copia al fine di garantirne l'integrità e la durata nel tempo. È previsto, in collegamento con NF Z 42-026, il sistema di riferimento per la certificazione NF 544 *Prestations de numérisation fidèle de documents sur support papier*, pubblicato nel 2018.

La prima versione dello standard risale al 1999, ma è stata revisionata nel 2009 e nel biennio 2018-2020. Questi aggiornamenti hanno permesso di estendere il campo di applicazione dello standard a tutti i tipi di media digitali, agli ambienti cloud e altri tipi di servizio, ampliando i requisiti di sicurezza informatica e includendo la trattazione dei dati personali. È stato tradotto in inglese e nel 2012, divenendo lo standard internazionale ISO 14641-1, ora pubblicato come ISO 14641:2018 *Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications*.

Dalla fine dello stesso anno, inoltre, è stata inoltre rilasciata da AFNOR la certificazione NF 461 - *Système d'archivage électronique pour compte de tiers*[53] che consente alle organizzazioni e alle aziende di verificare la conformità del proprio sistema di archiviazione elettronica ai requisiti di NF Z42-013 e per certificarne la conformità. Le *Règles de certification* prevedono l'inoltro di un'istanza all'ente certificatore AFNOR, il quale, dopo aver valutato il dossier fornito, effettua una procedura di audit, sulla matrice di NF Z42-013 – ISO 14641:2018 e GA Z42-019 *Guide d'application de la NF Z42-013*[54].

Référentiel Général de Gestion des Archives, d'interopérabilité e de Sécurité

Vi sono, poi, dei *Référentiels généraux* per la gestione, l'interoperabilità e la sicurezza relativi in particolare alla fase di gestione corrente degli archivi, che determinano però anche le caratteristiche dei documenti e dei dati custoditi negli archivi *intermédiaires* e *définitives*.

Il primo documento è il *Référentiel Général de Gestion des Archives* (R2GA): nell'ambito del CIAF, i ministeri della Cultura e della Comunicazione, della Difesa e degli Affari esteri hanno collaborato allo sviluppo di questo Quadro generale per la gestione degli archivi (R2GA), documento strategico che riferisce le linee guida sulla formazione, gestione e conservazione degli archivi. Partendo dalle definizioni di base, veicola informazioni sull'importanza di gestire correttamente gli archivi per garantire diritti, contribuire all'efficienza amministrativa e migliorare la qualità del patrimonio informativo e ne descrive

[53] V. *supra.*

[54] Le Regole di certificazione N 461, nella cui *Partie 2 - Le referentiel d'exigences* sono indicati tutti i requisiti richiesti dai citati riferimenti NF e GA NF Z42-013 – ISO 14641:2018 e GA Z42-019, sono scaricabili al link <http://cdn.afnor.org/download/reglements/FR/REGNF461.pdf> (ultima consultazione 03/02/2021).

il contesto, comprendendo la trattazione delle caratteristiche degli archivi pubblici, delle disposizioni penali a tutela di questi ultimi, della loro comunicazione, diffusione e diritto di accesso. Per quanto riguarda le indicazioni, fornisce un prospetto dei ruoli e delle responsabilità dei soggetti produttori di archivi pubblici (sia in relazione agli archivi 'correnti' e 'intermedi', sia in relazione agli obblighi di trasferimento degli archivi definitivi, distinti tra servizi e operatori statali e servizi degli enti locali, delle loro aggregazioni e enti pubblici). Vi sono poi definiti i ruoli e le responsabilità dell'amministrazione archivistica, ovvero svolgere attività di consulenza, perizie, audit e di controllo scientifico e tecnico degli archivi pubblici. Il documento si chiude con l'esposizione delle modalità di elaborazione di strategie e *policies* di conservazione, inquadrate nel contesto della governance delle informazioni e delle procedure attuabili (mutualizzazione ed esternalizzazione)[55].

Il *Référentiel général d'interopérabilité* (RGI)[56] è un *framework* che include norme e standard che promuovono l'interoperabilità tra i sistemi informativi della pubblica amministrazione. L'RGI è definito nell'ordinanza n ° 2005-1516 dell'8 dicembre 2005 relativa agli scambi elettronici tra utenti e autorità amministrative e tra autorità amministrative stesse[57]. La versione attualmente in vigore è la 2.0, formalizzata col decreto del 20 aprile 2016[58]: deve essere applicata ai collettivi territoriali, a tutti gli organismi pubblici (compresi quelli di ambito sociale e sanitario) e le amministrazioni centrali dello Stato (inclusi i loro servizi decentrati), al fine di incrementare l'efficienza dei servizi pubblici e la qualità della trasformazione digitale; fissa le regole dell'architettura e dei formati per i sistemi informativi pubblici senza imporre una soluzione unica, con l'obiettivo però di evitare la proliferazione di scelte eterogenee. Vi sono trattati gli scambi tra autorità amministrative, tra un'autorità amministrativa e un'impresa e tra un'autorità amministrativa e un cittadino, ciascuno in base ai livelli organizzativo, semantico e tecnico e di *policy* legali. L'RGI individua diversi profili di interoperabilità corrispondenti a effettivi casi d'uso di

[55] Il documento, aggiornato a ottobre 2013, è disponibile al link <https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2014/07/r2ga_document_complet_201310.pdf>.

[56] A proposito, si veda C. Sibille, *Une nouvelle version du Référentiel général d'interopérabilité*, «Hypotheses», 11 mai 2016, disponibile al sito <https://siaf.hypotheses.org/644>.

[57] Ordonnance n° 2005-1516 du 8 décembre 2005 *relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.* All'art. 11 il RGI fissa le regole tecniche che consentono di garantire l'interoperabilità dei sistemi informativi.

[58] Arrêté du 20 avril 2016 *portant approbation du référentiel général d'interopérabilité*.

integrazione. Per ciascuno di questi profili, l'RGI specifica una serie di standard e raccomandazioni. Il profilo per l'archiviazione digitale distingue tre categorie di formati: di gestione e scambio, per esigenze di interoperabilità immediata con sistemi di archiviazione, come SEDA, formati di diffusione e consultazione e formati di archiviazione, per la garanzia di conservazione a medio o anche a lungo termine[59].

È importante menzionare, in questa sede, il citato *Standard d'Échange de Données pour l'Archivage* (SEDA - standard di scambio dati per l'archiviazione), frutto di una collaborazione avviata nel 2006 tra gli Archivi di Francia e l'ex Direzione Generale per la Modernizzazione dello Stato (DGME): mira a facilitare l'interoperabilità tra il sistema informativo di un servizio di archivi e i sistemi informativi dei suoi partner per lo scambio di dati. Lo standard consente di modellare le transazioni (trasferimento, comunicazione, eliminazione, modifica e restituzione) tra diversi attori (soggetto produttore, servizio versante, servizio di archiviazione e utenti) nell'ambito del processo di archiviazione. Specifica i tipi, l'ordine e la forma dei messaggi scambiati, definendo quali metadati utilizzare per descrivere, gestire e perpetuare le informazioni. Sono state emesse diverse versioni dello standard dal 2006[60]: l'ultima emessa è la 2.1, pubblicata a giugno 2018[61].

Lo standard, tanto archivistico quanto tecnico, è strutturato in XML, utilizza la descrizione a più livelli degli standard ISAD-G e EAD, adotta il modello organizzativo ISO 14721 e la conservazione delle informazioni tecniche "trasportate" prende in prestito le definizioni di PREMIS. Nel 2012, il SIAF ha avviato il processo di standardizzazione SEDA con AFNOR dalla versione 1.0, poiché tale riconoscimento normativo veniva richiesto dai prestatori di servizi di archiviazione in esternalizzazione e da altri enti, quali banche: ne è conseguita la pubblicazione nel 2014 della norma NF Z 44-022 *Modélisation des Échanges de DONnées pour l'Archivage* (MEDONA - Modellazione degli scambi di dati per l'archiviazione), cui la versione 2.0 di SEDA è compatibile. Il processo è proseguito con il riconoscimento di MEDONA come standard internazionale, per poter ampliare il perimetro

[59] Sono menzionati, a tal proposito, PDF/A, ODF, XML, ZIP, TAR, FLAC, MIME.

[60] Versione 0.1 marzo 2006, versione 0.2 gennaio 2010, versione 1.0 settembre 2012, versione 2.0 (conforme allo standard MEDONA) dicembre 2015.

[61] I comitati SEDA si sono fermati nel 2018, dopo la pubblicazione della versione 2.1. Nel 2019, le esperienze di utilizzo di SEDA hanno portato all'emergere di punti in cui la versione 2.1 necessita di miglioramento, di cui si terrà conto nella successiva edizione.

di azione ad altri soggetti responsabili della conservazione digitale, pubblici e privati: nel 2017 è stato pubblicato come ISO 20614:2017 *Information and documentation — Data exchange protocol for interoperability and preservation*[62].

Il terzo quadro di riferimento è il *Référentiel Général de Sécurité* (RGS), per la sicurezza dei sistemi informativi. Elaborato dall' *Agence nationale de la sécurité des systèmes d'information* (ANSSI - Agenzia Nazionale per la Sicurezza dei Sistemi Informativi) e dall'allora *Direction interministérielle du numérique et du système d'information et de communication* (DINSIC Direzione Interministeriale per i Sistemi Digitali e di Informazione e Comunicazione[63]), si rivolge alle autorità amministrative e i loro fornitori di servizi. Ha lo scopo di garantire l'integrità e la protezione dall'esposizione a rischi dei dati condivisi tra le pubbliche amministrazioni, stabilendo i requisiti di sicurezza a cui le autorità amministrative devono conformarsi per la protezione dei i dati, in particolare sensibili, che questi enti utilizzano e scambiano, sia nei rapporti reciproci sia con altre organizzazioni o utenti. La versione 2.0 del documento, pubblicata nel 2014, sostituisce la prima versione pubblicata nel 2010: si tratta di una versione transitoria, che verrà sostituita da una terza versione che tiene conto della normativa europea in materia di protezione dei dati personali[64]. Si delinea, comunque, una metodologia orientata alla responsabilità delle autorità nei confronti dei loro sistemi informativi (analisi dei rischi e definizione degli obiettivi di sicurezza) e contiene regole e best practices che le amministrazioni devono mettere in atto quando si avvalgono di servizi specifici (ad esempio, certificazione elettronica e marca temporale, audit di sicurezza). Comprende le norme che consentono alle autorità amministrative di garantire ai cittadini e alle altre amministrazioni un livello di sicurezza dei propri sistemi informativi adeguato alle sfide e ai rischi associati alla sicurezza informatica: si descrivono le fasi di implementazione dei sistemi di sicurezza, la crittografia e protezione degli scambi elettronici, la qualificazione di prodotti di sicurezza e fornitori di servizi fiduciari e la convalida dei certificati da parte dello Stato[65].

---

[62] A proposito, si veda <https://francearchives.fr/fr/article/88482501> (ultima consultazione 03/02/2021) Lo standard SEDA e la documentazione associata sono disponibili su un sito dedicato <https://www.francearchives.fr/seda/index.html>.

[63] Ora DINUM; si veda il paragrafo III.3.2.

[64] Reg. UE 2016/679.

[65] Il documento, aggiornato al 2014, è disponibile al link < https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf >.

III.4 Olanda[1]

III.4.1 Introduzione

Il contesto olandese mostra grande attenzione per gli aspetti connessi alla conservazione dei documenti digitali.

Innanzitutto, l'ambito normativo è appannaggio del Ministero dell'Istruzione, della Cultura e della Scienza, che si occupa anche di fornire linee guida e strumenti a sostegno di uno sviluppo di politiche e sistemi coerente, uniforme e al passo con le innovazioni.

Dal punto di vista normativo, si sta assistendo a un aggiornamento della normativa primaria di settore: la Legge archivistica risale al 1995 e contiene, prevalentemente, disposizioni relative all'ambito analogico; la proposta di legge 2021 mira ad adeguare il contenuto della norma alla produzione di documenti digitale, tenendo conto in particolare del venir meno della componente 'fisica' degli archivi e delle conseguenze in termini di responsabilità e titolarità sui documenti.

Del corredo normativo in materia di archivi fanno parte anche il Decreto sugli archivi del 1995 e il Regolamento sugli archivi: entrambi stanno affrontando lo stesso percorso di rinnovamento della Legge sugli archivi, ma il secondo presenta già elementi che approfondiscono le modalità appropriate di mantenimento delle memorie digitali. In particolare, si definiscono gli aspetti legati alle modalità di tenuta della documentazione, della metadatazione e delle eventuali migrazioni.

L'approccio nei confronti dei modelli è di apertura al contesto internazionale: l'e-Depot, sistema progettato per la conservazione della documentazione digitale del governo olandese, utilizza strumenti *open source* implementati dalla comunità internazionale, nell'ottica di disporre di una soluzione che si basa su tecnologie condivise e che beneficiano dei *feedback*

[1] La bibliografia e le risorse telematiche per il contesto olandese sono state reperite attraverso i contatti con Remco van Veenendaal, responsabile della conservazione presso gli Archivi Nazionali, e attraverso il Servizio Informazioni al Pubblico del Governo Olandese. Si segnalano, inoltre, i riferimenti dei principali siti web istituzionali consultati: Nationaal Archief, visionabile al link <https://www.nationaalarchief.nl/> *Inspectie Overheidsinformatie en Erfgoed*, visionabile al link <https://www.inspectie-oe.nl/ >, *Rijksoverheid*, visionabile al link <https://www.rijksoverheid.nl/>.

di un ampio bacino di utenti. Tale attitudine è confermata anche dall'azione del Forum sulla standardizzazione, tramite cui avviene il confronto con l'ambito europeo.

III.4.2 Conservazione digitale e contesto amministrativo: organismi al coordinamento delle politiche sugli archivi

In Olanda il principale organo entro le cui competenze si trovano le questioni relative alla conservazione digitale è il *Ministerie van Onderwijs, Cultuur en Wetenschappen* (Ministero dell'Istruzione, della Cultura e della Scienza); in misura minore, è coinvolto il *Ministerie van Economische Zaken en Klimaat* (Ministero per gli Affari economici e le politiche ambientali).

Ministerie van Onderwijs, Cultuur en Wetenschappen

Il Ministero dell'Istruzione, della Cultura e della Scienza ai occupa delle questioni relative alla conservazione dei documenti attraverso l'*Inspectie Overheidsinformatie en Erfgoed* (Ispettorato per l'informazione e il patrimonio culturale). In linea generale, l'Ispettorato è un organismo indipendente che assicura il rispetto della legge, sulla cui qualità ed efficacia fornisce consulenza e promuove il miglioramento della gestione e della cura del patrimonio culturale. Nello specifico, poi, la divisione *Overheidsinformatie* (Informazione) sovrintende alla creazione, gestione e conservazione dei *records* pubblici del governo centrale[2]: si occupa della vigilanza sugli archivi, monitorando la registrazione, l'accessibilità, l'archiviazione sicura e permanente, la selezione e la distruzione del materiale archivistico e assicurando che gli archivi selezionati per la conservazione a lungo termine siano correttamente elaborati e trasferiti agli archivi pubblici come beni culturali; a tal fine effettua

[2] A livello nazionale, l'Ispettorato dell'Informazione Pubblica e del Patrimonio supervisiona la gestione degli archivi del governo centrale: questi includono gli alti organi dello Stato (come il Consiglio di Stato), i ministeri e tutti i loro dipartimenti e istituzioni (compresi quelli delle province), gli organi di PBO (come i Consigli sui prodotti di mercato) e gli organi amministrativi indipendenti come le università e, ad esempio, il catasto e la Autorità dei mercati finanziari. A tal fine, l'Ispettorato delle informazioni e del patrimonio del settore pubblico conduce indagini, effettua ispezioni e fornisce informazioni sul rispetto della legislazione sugli archivi: supervisori provinciali in questo settore collaborano nella consultazione nazionale degli ispettori provinciali degli archivi (LOPAI). In base alle leggi sui comuni, le province supervisionano l'attuazione delle norme presso i comuni e gli enti idrici, comprese quelle sugli archivi. Le province possono intervenire con in caso di inadempienze (si veda, in proposito, il sito dedicato alla vigilanza sugli archivi <https://www.archiefinspecties.nl/>).

ispezioni presso le organizzazioni stesse, verificando l'intera gestione rispetto alla normativa archivistica, oppure concentrandosi su aspetti specifici.

A conferire le funzioni di vigilanza al Ministero dell'Istruzione e a delegarle all'Ispettorato è l'*Archiefwet* (Legge sugli archivi)[3]: questa stabilisce, in primo luogo, che il Senato e la Camera dei Rappresentanti degli Stati Generali, gli altri Alti Consigli di Stato, il Direttore del Gabinetto del Re e il Ministero dell'Istruzione si occupano dei propri documenti sino al trasferimento in un archivio di stato e i commissari provinciali sono responsabili . Il Ministero dell'Istruzione subentra nella responsabilità nel momento in cui i documenti sono conservati negli archivi di stato; per quanto riguarda 1'ambito provinciale è la dirigenza di quest'ultima a essere responsabile della gestione e conservazione dei documenti degli organi provinciali, sulla base di un ordinanza del relativo Consiglio, mentre per i comuni sono il sindaco e gli assessori sono responsabili dell'archiviazione degli atti degli organi comunali, con ordinanza da adottarsi in Consiglio comunale e comunicata alla giunta provinciale[4].

Sotto la responsabilità politica di questo Ministero dell'Istruzione, della Cultura e della Scienza sono anche i *Nationaal Archief*, gli Archivi Nazionali d'Olanda (NANETH – *National Archives of Netherlands*)[5], il cui direttore riporta direttamente al direttore generale della Cultura e dei Media entro il Ministero stesso. Il loro scopo, delineato nella stessa *Archiefwet*, consiste nel gestire le collezioni di documenti nazionali e svolgere attività tali da costituire e mantenere un solido sistema archivistico, perseguito attraverso l'utilizzo di opportune *policies* per la selezione e lo scarto della documentazione. La stessa legge assegna agli Archivi Nazionali il ruolo di deposito centrale per la conservazione dei documenti delle autorità amministrative statali, le quali, come già visto, sono a loro volta obbligate a tenere la propria documentazione in buone condizioni, adeguatamente sistemata e accessibile.

Gli Archivi Nazionali si occupano inoltre di fornire supporto sulla sostenibilità digitale per istituzioni archivistiche, enti governativi e terze parti: un punto importante della loro

[3] Archiefwet 1995 *wet van 28 april 1995, houdende vervanging van de Archiefwet 1962 (Stb. 313) en in verband daarmede wijziging van enige andere wetten* (*AW 1995*).

[4] Artt. 23, 24, 25-bis, 27, 30 AW 1995.

[5] L'istituzione degli Archivi Nazionali d'Olanda risale al 1802, momento in cui l'Olanda si trovava sotto l'influenza napoleonica. La centralizzazione della struttura all'Aia ad opera di re Guglielmo I ha avuto luogo nel 1814, data da cui custodiscono la documentazione relativa alle attività amministrative degli organi centrali dello stato (Franks, Bernier (a cura di), *The international directory of national archives*, cit., pp. 268-271).

mission è costituito dal monitoraggio e dal continuo aggiornamento sulle nuove tecnologie e i nuovi sviluppi; a tal proposito, i *Nationaal Archief* hanno implementato e curano l'e-Depot, il cuore dell'infrastruttura digitale dedicata alla conservazione dei documenti elettronici dell'apparato amministrativo statale[6].

Per quanto attiene alla concreta collocazione di tale rete di archivi, all'Aia si trova il Deposito generale dell'Archivio di Stato, destinato alla custodia dei *records* degli organi di governo le cui funzioni si estendono o si sono estese a tutto lo Stato e il cui archivista di stato generale è amministratore. Nel capoluogo di ciascuna provincia si trova, invece, una sede separata di Archivio di Stato, destinata alla custodia degli atti degli organi nazionali istituiti in quella provincia, delle ex amministrazioni provinciali e dipartimentali e degli organi di governo le cui funzioni non si estendono o si sono estese a tutta la nazione: l'amministratore è un archivista di Stato in possesso di idoneo titolo in scienze archivistiche[7].

Ministerie van Economische Zaken en Klimaat

Questo Ministero ha incidenza tangenziale sul tema della conservazione digitale in quanto è l'organismo competente in materia di digitalizzazione degli apparati statali.

Si occupa, in particolare, della direzione delle politiche digitali e della programmazione della relativa agenda per il settore ICT; a tal proposito, ha avviato le attività del *Forum Standaardisatie*[8], la cui costituzione ha avuto come obiettivo il coordinamento dell'e-government e la scelta degli standard e delle linee guida più appropriate nell'ottica dell'interoperabilità.

III.4.3 Disposizioni sulla conservazione dei documenti e degli archivi digitali

Le disposizioni generali in materia di conservazione di documenti sono contenute nella Legge sugli archivi del 1995, integrata dal Decreto sugli archivi del 1995 e dal Regolamento sugli archivi.

[6] Si veda, in proposito, il paragrafo III.4.4.
[7] Art. 26 *AW 1995*.
[8] Si veda, in proposito, il paragrafo III.4.4.

È, attualmente, in corso di approvazione un aggiornamento di questa norma, finalizzato all'adattamento al contesto digitale.

Archiefwet

L'*Archiefwet* del 1995 (Legge sugli archivi) contiene le norme volte a far sì che il governo conservi le proprie informazioni in modo adeguato, nella consapevolezza dell'importanza sia di stabilire prescrizioni per la gestione operativa del governo stesso, sia per responsabilità pubblica e prospettiva storico-culturale.

In primo luogo, è demandato agli organi governativi stessi l'obbligo di conservare in buono stato e in maniera ordinata e accessibile i documenti archivistici da essi detenuti, così come di assicurare la distruzione degli atti da scartare[9]. A tal proposito, viene disposto che l'autorità responsabile è tenuta a redigere liste di disposizione in cui sia indicato almeno quali documenti possano essere distrutti[10]; tali liste vengono approvate in maniera differente, a seconda della tipologia di documentazione prodotta: per i documenti d'archivio del Senato e della Camera dei Rappresentanti degli Stati Generali, degli altri Alti Consigli di Stato e del Gabinetto del Re è previsto un Regio Decreto, su proposta del Ministro dell'Istruzione d'intesa con l'organo di governo interessato; per i documenti dei ministeri e di altri organi di governo è previsto il benestare del Ministro dell'Istruzione e dagli altri Ministri interessati. La formalizzazione di un elenco di selezione è pubblicata nella Gazzetta ufficiale olandese[11].

In ogni caso, il Ministero può procedere con la distruzione dei documenti conservati in un archivio statale soltanto dopo aver ricevuto l'autorizzazione del responsabile per il cui ordine i documenti sono stati trasferiti[12].

---

[9] Art. 3 *AW 1995*. Interessante, in proposito, anche l'art. 4 *AW 1995*, che prevede, in caso di cessazioni, scissioni, modifiche o istituzioni provvisorie di enti pubblici, che vengano sempre prodotte disposizioni relative agli archivi e alla destinazione della documentazione.

[10] In tali elenchi di selezione l'ente governativo responsabile indica quali categorie di documenti si qualificano per l'archiviazione permanente e quali saranno distrutti dopo la scadenza del periodo di conservazione.

[11] Art. 5 *AW 1995*. Tali elenchi di scarto sono consultabili al link <https://www.nationaalarchief.nl/archiveren/zoeken?activeTab=archive&qf_type_item_term_name=Selectielijst&resultsPerPage=50>.

[12] Art. 6 *AW 1995*. Riguardo al versamento, l'art. 12 impone all'autorità responsabile il trasferimento dei documenti di archivio che non possono essere distrutti e che hanno più di vent'anni nella competente struttura archivistica, con modalità stabilite in base a un'ordinanza in Consiglio. L'art. 13 prevede, in aggiunta, che i documenti che hanno meno di vent'anni possano essere versati se la figura di riferimento dell'archivio in cui verranno depositati ritiene vi siano motivi validi, mentre atti aventi più di vent'anni, al contrario, possono essere

Poiché la legislazione attuale si concentra principalmente sul cartaceo, la legge sugli archivi sta subendo un iter di modifica, in atto dal 2018, per poter essere adattata agli sviluppi digitali: si prevede che il testo della nuova disposizione entri in vigore tra la fine del 2022 e l'inizio del 2023, avendo superato la fase di consultazione e ottenuto l'approvazione da parte del Consiglio dei Ministri ed essendo attualmente sottoposta al parere del Consiglio di Stato[13]. La finalità di questo aggiornamento è prevedere la conservazione permanente delle informazioni pubbliche sia in formato cartaceo sia in formato digitale, in modo da disporre di archivi adeguati alle innovazioni e trasparenti. In questo contesto è stata semplificata la disciplina statutaria degli archivi di Stato: invece di un archivio generale degli archivi di stato e di undici diversi archivi di stato, questo disegno di legge prevede un regolamento per un archivio digitale nazionale, sotto la responsabilità del Ministero dell'istruzione, della Cultura e della Scienza, incaricato della conservazione e della disponibilità permanenti di documenti provenienti dagli organi del governo.

Nello specifico, la Legge sugli archivi del 1995 ha una settorializzazione direttamente correlata alla struttura del governo e ai suoi livelli amministrativi, mentre la proposta di modifica, piuttosto che la provenienza dei documenti, concepisce come chiave di volta per l'organizzazione delle disposizioni il 'corso di vita' dei documenti: conseguentemente, gli articoli hanno subito, oltre alla modifica nel contenuto, una riorganizzazione in base a questo criterio logico[14].

tenuti presso il soggetto produttore qualora siano ancora frequentemente utilizzati o consultati, dietro autorizzazione a sospendere il trasferimento dal Ministro dell'Istruzione.

[13] Il disegno di legge è stato presentato con la denominazione *Voorstel van Wet tot intrekking van de Archiefwet 1995 en vervanging door de Archiefwet 2021 (Archiefwet 2021 – AW 2021)*. Sulle novità introdotte dalla proposta di rinnovo della Legge archivistica del 1995, si vedano la relazione esplicativa alla modifica pubblicata al link <https://www.internetconsultatie.nl/1574> e la sezione del sito istituzionale del *Nationaal Archief* <https://www.nationaalarchief.nl/archiveren/kennisbank/nieuwe-archiefwet-2021>.

[14] Si riportano i titoli della Legge sugli Archivi del 1995 e della proposta 2021, al fine di mostrare l'evidenza della nuova organizzazione. Per quanto riguarda il provvedimento del 1995, l'indice è composto da: Capo I. Disposizioni generali; Capo II. Documenti d'archivio in generale; Capo III. Archivi di Stato; Capo IV. Documenti d'archivio provinciali; Capo V. Archivi comunali; Capo VI. Documenti d'archivio dei *water board*; Capo VII. Documenti d'archivio di altri enti governativi; Capo VIII. Disposizione penale; Capo IX. Disposizioni transitorie e finali. Per quanto riguarda la proposta del 2021, questo si compone di: Capo 1. Disposizioni generali; Capo 2. Organi di governo responsabili; Capo 3. Gestione; Capo 4. Selezione, distruzione e trasferimento; Capo 5. Servizi archivistici e archivisti; Capo 6. Archivi pubblici e archivi pubblici riservati; Capo 7. Accesso agli archivi trasferiti; Capo 8. Disposizioni speciali per la gestione degli archivi trasferiti; Capo 9. Vigilanza ed esecuzione; Capo 10. Disposizioni transitorie e finali.

Altro cambiamento significativo si ha nella terminologia: sono state semplificate le definizioni, in modo tale da renderle più in linea con le prassi di gestione delle informazioni digitali e nel tentativo di creare un significativo collegamento con la nuova legge in materia di accessibilità delle informazioni di interesse pubblico[15], anch'esso ancora in discussione, attraverso la differenziazione degli elementi digitali e analogici e la generalizzazione delle denominazioni fondamentali per renderle adatte a entrambi i contesti[16].

Nel disegno di legge sono stati distinte quattro aree di interesse: la prima di ordine amministrativo e riguarda la possibilità di poter reperire e utilizzare le informazioni presenti negli archivi per le proprie attività istituzionali e di servizi ai cittadini e alle imprese; in secondo luogo, i documenti custoditi negli archivi rappresentano l'evidenza della responsabilità pubblica per le azioni del governo; in terzo luogo, gli archivi contengono documenti dai quali i governi stessi, i cittadini e le imprese possono trarre diritti e doveri e che possono svolgere funzione di prova nei casi giudiziari; infine, gli archivi governativi, nel momento in cui sono conservati in modo permanente, sono considerati parte del patrimonio culturale: costituiscono la memoria nazionale, fonte di ricerca e storiografia cui non solo possono fare riferimento gli studiosi, ma anche tutti i cittadini. Altri obiettivi chiave di cui la nuova legge sugli archivi tiene conto sono anche la politica olandese sui dati aperti, la relazione coerente con altre leggi, come quelle sull'accesso delle informazioni per il pubblico, il riutilizzo delle informazioni governative, la protezione dei dati personali e la considerazione dei servizi digitali.

Restano invariate le indicazioni sul mantenimento in buono stato, ordinato e accessibile dei documenti, ma si aggiunge l'imposizione per gli enti governativi dell'adozione di misure appropriate per garantire questi requisiti: queste devono essere organizzative e tecniche, stabilite in base alla valutazione proporzionale degli interessi amministrativi e storici dei documenti e al rischio di perdita delle informazioni[17].

---

[15] Si tratta del WOO, il *Voorstel van wet van de leden Snels en Van Weyenberg tot wijziging van het voorstel van wet van de leden Snels en Van Weyenberg houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid - Wijzigingswet Woo)*, ovvero il disegno di legge contenente norme sull'accessibilità delle informazioni di interesse pubblico che andrà a sostituire il vigente WOB, ovvero il *Wet van 31 oktober 1991, houdende regelen betreffende de openbaarheid van bestuur (Wet openbaarheid van bestuur)*.

[16] Artt. 1.1 *AW* 2021.

[17] Art. 3.1 *AW* 2021.

Queste indicazioni si relazionano agli aspetti connessi alla redazione degli elenchi di selezione[18]: anche con l'introduzione del digitale, sono ritenuti uno strumento importante, in quanto coostituiscono una base giuridica per l'archiviazione permanente o la distruzione dei documenti. Con il rinnovo della legge 2021, si semplifica la procedura di redazione: si prevede un metodo uniforme e più semplice, che vede l'intervento del Ministro dell'Istruzione, della Cultura e della Scienza, d'intesa con l'organo di governo interessato. Nello specifico, nel Decreto Archivi modificato decade l'applicazione della procedura di discussione pubblica: i progetti di decisione non devono più essere messi a disposizione in revisione per un periodo di sei settimane. La soppressione di questa procedura preparatoria non altera il fatto che l'adozione dell'elenco di selezione è una decisione ai sensi della legge sul diritto amministrativo generale: è pubblicata nella Gazzetta Ufficiale, e, di conseguenza, nota a tutti e soggetta a ricusazione e ricorso. Nello stesso decreto si stabilisce anche una validità di questo documento per dieci anni: il dimezzamento di tale periodo rispetto alla legge del 1995 è in linea con la riduzione del termine di versamento della documentazione per la conservazione. Allo stesso tempo, viene definito che l'elenco di selezione rispecchi a quali tipi di applicazioni e sistemi è rivolto: si sostituisce la prevalenza della struttura organizzativa con la modalità di gestione delle informazioni.

Questo disegno di legge mantiene l'obbligo di distruzione dei documenti sulla base degli elenchi di selezione e aggiunge che gli enti governativi adotteranno misure appropriate a tal fine: vengono dettagliate ulteriormente le casistiche di cancellazione delle informazioni, distinguendo i casi dei dati aperti, in relazione ai quali viene definito sufficiente il diniego dell'accesso, dei dati personali o dei documenti speciali da cui terze parti non possono più derivare diritti, per cui si opta per l'eliminazione dei file, mentre per le informazioni riservate non destinate all'archiviazione permanente viene presa in considerazione anche la distruzione dell'hardware. Non cambia quanto stabilito nella Legge sugli archivi del 1995 sulla dichiarazione di distruzione, che contiene almeno una specificazione dei documenti eliminati e i relativi metodi di cancellazione e che rappresenta uno strumento per attribuire la responsabilità di queste operazioni.

[18] Art. 4.1 *AW* 2021.

Altra importante novità riguarda la riduzione dei tempi di versamento dei documenti per il governo centrale, i comuni e gli altri enti a dieci anni invece di venti, consentendo ai ricercatori accesso anticipato ai dati[19]: le informazioni che vanno conservate in modo permanente raggiungono prima gli archivi pubblici, presso cui sono gestite in modo sostenibile e accessibili gratuitamente e, fatte salve le restrizioni inerenti al contenuto, sono liberamente consultabili; inoltre, questa riduzione viene interpretata anche come un incentivo ad attuare coi tempi opportuni misure tali da disporre di *records* ben ordinati, col corretto set di metadati e predisposti alla conservazione a lungo termine. Interessante un punto del dibattito sulla legge riguardo alla superfluità nell'ambito digitale di stabilire tempistiche di versamento in conservazione dei documenti, che però non è stato accolto in quanto rappresentano un cardine per l'applicazione del regime giuridico archivistico, che comprende la valutazione e la selezione, l'accesso del pubblico e le regole per l'utilizzo delle informazioni, e un importante *terminus post quem* per il passaggio di responsabilità amministrativa sugli archivi dagli organi centrali del governo al Ministero dell'Istruzione, della Cultura e della Scienza[20].

Come la Legge sugli archivi del 1995, questo disegno prevede la possibilità di posticipare, motivatamente, il trasferimento a un servizio di archivio di 10 anni o di effettuare tale operazione anticipatamente, in accordo con il soggetto che cura la conservazione. Vi è, invece, una novità che riguarda l'inserimento di un'opzione di esenzione speciale per il mantenimento dei documenti presso il soggetto produttore: si applica a un numero limitato di organizzazioni governative, per cui la tipologia dei file non è in linea con i principi di conservazione permanente adottati su larga scala o l'utilizzo dei documenti è necessario per lo svolgimento di attività correnti. La ragione di tale scelta sta nella tutela del mantenimento dell'integrità dei dati e nella salvaguardia dei compiti statutari dell'ente pubblico, fermo restando l'obbligo da parte di quest'ultimo di preservare il buono stato, ordinato e accessibile dei documenti e di provvedere adeguatamente alla loro conservazione permanente e alla disposizione di strumenti per la fruizione al pubblico[21].

[19] Art. 4.3 *AW 2021*.

[20] Nel caso delle autorità decentrate, la responsabilità dell'archivio resta in capo all'ente governativo competente.

[21] Artt. 4.5 *AW* 2021.

Al di là delle eccezioni ammesse, vi sono degli aspetti connessi al regime d'accesso interessate da questa modifica: infatti, i limiti temporali imposti alla consultabilità dei documenti in relazione alla natura del contenuto potrebbero essere più estesi del decennio individuato. Questa circostanza sarà risolta con l'applicazione di restrizioni temporanee all'accesso pubblico e con la possibilità di visualizzare soltanto le parti di documento non interessate da dati particolari[22]. Ciò avviene in allineamento con il *Wet openbaarheid van bestuur* (WOB – Legge sulle informazioni governative e l'accesso al pubblico): per le motivazioni sulla restrizione è stato individuato un collegamento l'articolo 10 del WOB[23], in modo tale che queste condizioni vengano specificate e approfondite in modo tale da semplificare il coordinamento e la comunicazione tra soggetto produttore dell'archivio e l'amministratore del servizio archivio, consentendo inoltre la possibilità di elaborare le indicazioni per la divulgazione nei sistemi informativi *by design* e di facilitare la gestione degli accessi alla documentazione da parte del pubblico[24].

In relazione all'organizzazione dell'Archivio di Stato e delle reti periferiche, il nuovo disegno di legge tiene conto del fatto che il versamento dei documenti digitali non implica più conseguenze dal punto di vista fisico: la documentazione degli organi di governo

[22] Artt. 6.1-6.7 *AW* 2021.

[23] Art. 10 WOB «1. La consultabilità delle informazioni ai sensi della presente legge è esclusa nella misura in cui: A. metta in pericolo l'unità della Corona; B. possa nuocere alla sicurezza dello Stato; C.riguardi dati aziendali e produttivi, comunicati in via riservata al Governo da persone fisiche o giuridiche; D. dati personali di cui agli articoli 9, 10 e 87 del GDPR, a meno che la disposizione non violi apparentemente la privacy. 2. La comunicazione delle informazioni ai sensi della presente legge è altresì esclusa nella misura in cui l'interesse delle stesse non prevalga sui seguenti: A. le relazioni dei Paesi Bassi con altri Stati e con organizzazioni internazionali; B. gli interessi economici o finanziari dello Stato, degli altri organismi di diritto pubblico o delle autorità amministrative di cui all'articolo 1 bis, lettere c e d; C. l'indagine e il perseguimento di reati penali; D. ispezione, controllo e vigilanza da parte degli organi amministrativi; E. rispetto della privacy; F. l'interesse che il destinatario ha di essere il primo a essere informato dei dati; G. la prevenzione di vantaggi o svantaggi sproporzionati di persone fisiche o giuridiche o di terzi coinvolti nella questione. 3. Il secondo comma, incipit e sub E., non si applica nella misura in cui l'interessato abbia acconsentito alla divulgazione. 4. Il primo comma, incipit e sub C. e D., il secondo comma, incipit e sub E., e il settimo comma, incipit e sub A., non si applicano per quanto riguarda le informazioni ambientali relative alle emissioni. Inoltre, nonostante il primo comma, le parole iniziali e la lettera c., la consultazione di informazioni ambientali è esclusa solo nella misura in cui l'interesse alla divulgazione non prevalga sull'interesse ivi dichiarato. 5. Il secondo comma, incipit e sub B., si applica alla consultazione di informazioni ambientali nella misura in cui si tratti di atti di natura riservata. 6. Il secondo comma, incipit e sub G., non si applica alla consultazioni di informazioni ambientali. 7. Si omette anche la consultazione di informazioni ambientali ai sensi della presente legge nella misura in cui la sua importanza non prevalga sui seguenti interessi: A. la protezione dell'ambiente cui si riferiscono queste informazioni; B. la sicurezza delle aziende e la prevenzione dei sabotaggi. 8. Se non si applica il quarto comma, prima frase, quando si applicano il primo, il secondo e il settimo comma alle informazioni ambientali, si terrà conto del fatto che tali informazioni si riferiscano alle emissioni nell'ambiente».

[24] Artt. 7.1-7.6 *AW* 2021.

provinciale o di enti le cui funzioni non si estendono o si sono estese a tutto il regno confluisce in e-Depot, servizio di archiviazione sviluppato dall'Archivio Nazionale[25]. Dunque, il progetto è di disporre di un servizio archivistico nazionale centralizzato destinato alla conservazione permanente dei documenti del governo, gestito dall'archivista generale dello Stato: questo determina un efficientamento dal punto di vista dell'organizzazione dei trasferimenti e della messa in disponibilità delle risorse al pubblico.

Interessante menzionare anche una novità introdotta in merito alla formazione degli archivisti: non è più obbligatorio il diploma in scienze archivistiche per svolgere la funzione di archivista, ma si pone l'attenzione sull'esigenza di competenze in materia ITC e di coordinamento con esperti in altre discipline. Le conoscenze archivistiche vengono reputate necessarie ma, da sole, non più sufficienti: si amplia, pertanto, il range di corsi adeguati all'esercizio di tale funzione e si introduce la valutazione dell'idoneità alla nomina di archivista per il governo[26]. Si è proposto, in sede di discussione, di subordinare il conferimento del ruolo a una certificazione, ma è stato concluso che questo requisito avrebbe rappresentato la sostituzione di un obbligo con un altro e un contrasto rispetto alla volontà di estensione trasversale delle conoscenze e delle competenze.

Questi cambiamenti si relazionano con un'ulteriore novità: la nomina di un archivista sarà obbligatoria, mentre ai sensi della legge sugli archivi del 1995 la gestione degli archivi delle province, dei comuni o degli enti idrici poteva essere esercitata anche dal segretario.

Per quanto riguarda la vigilanza sulla documentazione, *l'Archiefwet* distingueva tra la fase precedente al versamento in archivio per la conservazione a lungo termine e la fase post scarto sulla base dell'elenco di selezione: solo la prima fase rientrava in questa attività, mentre con il nuovo disegno di legge viene estesa anche alla successiva. Viene ritenuto, infatti, che i documenti digitali richiedano un monitoraggio intensivo e continuo, necessario per la fruibilità, l'accessibilità, la sicurezza e l'affidabilità delle risorse conservate nell'e-Depot. Per quanto riguarda gli archivi prodotti dal governo centrale, la responsabilità su di essi è del Ministro dell'Istruzione, della Cultura e della Scienza: dunque, funzionari appositamente designati da questo Ministro vigilano anche sui documenti che sono stati

[25] Artt. 5.1-5-2 *AW* 2021. Sull'e-Depot si veda il paragrafo III.4.4.
[26] Artt. 5.3, comma 4 *AW* 2021.

trasferiti all'Archivio nazionale. Per le autorità locali, questo compito è effettuato dal Consiglio designato, che resta responsabile sui documenti anche dopo il trasferimento[27].

Contestualmente all'iter del disegno di legge, il Ministero dell'Istruzione, della Cultura e della Scienza sta lavorando alla modifica del Decreto sugli Archivi e del Regolamento sugli Archivi, in coordinamento con il Ministero degli Interni, VNG, l'Unione delle commissioni idriche, l'IPO, l'Ispettorato per l'informazione e il patrimonio del governo e gli archivi nazionali. Questi documenti, come le versioni precedenti legate alla Legge del 1995, descrivono più in dettaglio come dovrebbe essere attuata la nuova legge ed entreranno in vigore contemporaneamente all'*Archiefwet* 2021.

Archiefbesluit* e *Archiefregeling

Con i due documenti appena citati si completa il quadro giuridico sugli archivi.

L' *Archiefbesluit* tratta le modalità attuative della Legge sugli archivi. In linea di principio, il decreto sugli archivi veicola gli stessi contenuti della legge sugli archivi, ma prevede norme più dettagliate: sono definite le regole sulla redazione e determinazione degli elenchi di selezione, sulla sostituzione dei documenti con riproduzioni, sulla cessione della proprietà di documenti governativi, sulla gestione dell'archivio, sulla formazione del personale e sui locali interessati. Non vi sono disposizioni direttamente legate agli archivi e ai documenti digitali.

L'Archiefregeling riguarda, invece, le indicazioni tecniche e le misure specifiche da adottare per il mantenimento a lungo termine dei documenti, per la loro tenuta ordinata e per la loro accessibilità. Si articola in sezioni dedicate agli aspetti generali, alla durabilità dei documenti archivistici, al loro stato ordinato e accessibile e alle norme generali e speciali per la costruzione e sistemazione dei locali archivistici e per la costituzione e disposizione degli archivi.

Nello specifico, il titolare della custodia dell'archivio è in primo luogo tenuto ad applicare un sistema di gestione qualità al fine di disporre di evidenze che testimonino l'adeguatezza del trattamento della documentazione[28]. Inoltre, si prevede che questi garantisca che si possa

[27] Artt. 9.1-9.5 *AW* 2021.
[28] Art. 16 *AR*.

determinare il contenuto, la struttura e la forma del *record* nel momento in cui questo è stato ricevuto o redatto dall'ente governativo cui fa capo, chi è l'autore, in che data sia stato creato e in relazione a quale procedimento, quale sia il legame con gli altri documenti, come siano stati gestiti e i software eventualmente impiegati[29].

Il titolare, inoltre, assicura che gli organi di governo di sua competenza dispongano di un quadro aggiornato, completo e logicamente coerente degli atti archivistici detenuti da tale organo di governo, disposti secondo la struttura organizzativa applicabile al momento della creazione dell'archivio, tenendo traccia delle variazioni[30].

È previsto che si utilizzi, per i metadati a corredo di ciascun documento, lo stardard NEN-ISO 23081:2006[31]: questi devono essere funzionali a garantire l'accessibilità del documento, che, allo stesso tempo, deve essere leggibile e utilizzabile[32].

Per quanto riguarda gli archivi digitali, vi è dedicato l'intero paragrafo 2, contenente le *Norme speciali per la conservazione degli archivi digitali*.

Vi si determina che il titolare alla custodia dell'archivio debba monitorare l'usabilità dei documenti digitali e che i requisiti funzionali di ciascuno di essi siano tracciati per il contenuto, la struttura, la forma e il comportamento, nella misura in cui ciò sia necessario per garantire l'autenticità delle registrazioni digitali[33]. È necessario che, sulla base del quadro che descrive la struttura dell'archivio, possano essere individuati tutti i file informatici presenti e che questi contengano tra i metadati informazioni sulla loro natura tecnica originaria, ovvero ambienti hardware e software di creazione, le caratteristiche attuali – in modo tale che sia possibile effettuarne la riproduzione e, nel caso vi sia apposta una firma elettronica, il titolare della sottoscrizione, la convalida, il responsabile di tale convalida e l'identificazione del certificato[34].

Qualora vi sia probabilità che, a seguito di modifiche o a causa dell'obsolescenza, i software non possano più soddisfare i requisiti previsti dal Regolamento in merito allo stato

[29] Art. 17 *AR.*
[30] Art. 18 *AR.*
[31] Si veda, in proposito, il capitolo I.3.
[32] Artt. 19-20 *AR.*
[33] Artt. 21-22 *AR.*
[34] Artt. 23-24 *AR.*

di accessibilità e di tenuta ordinata delle scritture dell'archivio digitale, il titolare della custodia assicurerà che avvenga la conversione o la migrazione di tali atti elettronici, facendo sì che tali atti informatici possano essere utilizzati o consultati mediante emulazione secondo le modalità attuate momento della ricezione o della predisposizione da parte dell'ente governativo. Questi redige un verbale di conversione o migrazione, che contiene almeno la specificazione dei file che sono stati convertiti o migrati e che indica come e con quale esito è stato verificato tale operazione sia stata effettuata in modo tale da soddisfare i requisiti previsti dal Regolamento il relazione al mantenimento dello stato ordinato e accessibile[35].

È previsto, inoltre, che i formati utilizzati per la conservazione dei file siano validabili e completamente documentati, in conformità alla definizione di standard aperti, a meno che non sia possibile per la natura del documento, caso in cui si procede con la valutazione per il trasferimento su un formato di file alternativo. Qualora al momento della conversione venga utilizzata la tecnologia di cifratura, la corrispondente chiave di decrittazione sarà fornita al gestore del deposito dell'archivio. L'utilizzo della compressione è consentito solo nella misura in cui ciò non comporti una perdita di informazioni tale da non consentire più il rispetto dei requisiti previsti dal Regolamento in merito allo stato accessibile e ordinato dei documenti dell'archivio digitale[36].

Viene trattata infine la 'sostituzione' con riproduzioni: il titolare della custodia deve assicurare che vi siano evidenze sull'ambito del processo di copia, che comprende comunque l'indicazione delle unità documentali e delle categorie cui si applica questa procedura, degli strumenti, del software e delle impostazioni con cui viene effettuata, dei criteri di selezione per la riproduzione a colori, in scala di grigi o in bianco e nero, delle modalità di realizzazione della riproduzione, che comprende comunque i formati, le operazioni, i metadati e, se del caso, la scelta in merito alla riproduzione per lotto o per pezzo, delle misure per il controllo per la rappresentazione coerente e completa e della correzione degli errori, del processo di distruzione dei *record* sostituiti e delle garanzie di qualità[37].

[35] Art. 25 *AR*.
[36] Art. 26 *AR*.
[37] Art. 26-bis e ter *AR*.

Per quanto riguarda il progetto di rinnovamento con l'*Archiefwet* 2021, è interessante l'intento di ampliare il Regolamento con ulteriori disposizioni per i depositi elettronici per la conservazione permanente degli archivi trasferiti. Verranno aggiunti standard NEN e ISO al fine di stabilire il perimetro univoco di concetti e definizioni entro cui collocare le politiche per la conservazione, i metadati, i diritti e l'accesso e al fine di disporre di requisiti da soddisfare per garantire autenticità, affidabilità, integrità e usabilità dei documenti; in sede di adeguamento del Regolamento dell'Archivio si attingerà, inoltre, alla *roadmap* per la sostenibilità degli archivi tracciata dal *Netwerk Digitaal Erfgoed*[38], che a sua volta si basa su diversi strumenti di certificazione internazionali[39]. Non si indicheranno certificazioni obbligatorie, al fine di non inserire ulteriori oneri amministrativi e in quanto si ritiene che non offrano vantaggi rispetto agli strumenti di autovalutazione volontaria.

È interessante menzionare, in anticipazione al paragrafo seguente, che l'articolo 2 del Regolamento equipara i requisiti tecnici in esso stabiliti a quelli determinati in un altro Stato membro dell'Unione europea, in uno stato che è parte degli accordi sullo Spazio economico europeo, o in Turchia, che contengano eguali garanzie[40].

III.4.4 Modelli e standard di conservazione

e-Depot

L'e-Depot è l'archivio digitale sviluppato nell'ambito dell'Archivio Nazionale finalizzato a raccogliere le informazioni digitali provenienti da tutti i ministeri e dalle organizzazioni del governo centrale che operano a livello nazionale (come organi amministrativi indipendenti, organizzazioni esecutive e Alti Consigli di Stato), dalle istituzioni governative che trasferiscono i propri archivi ai Centri storici regionali e dalle attività di digitalizzazione degli archivi cartacei esistenti. I documenti saranno pubblicamente accessibili e utilizzabili attraverso i siti web degli Archivi nazionali e dei centri storici regionali, eccetto per quelli contenenti informazioni riservate o dati sensibili.

---

[38] Si veda, in proposito, il paragrafo III.4.4.

[39] Il documento, dal titolo *Naar een geharmoniseerde meting van gebruik en impact van digitaal erfgoed: een Plan van Aanpak* (Verso una metrica armonizzata per l'utilizzo e impatto del patrimonio digitale: un piano d'azione) <https://netwerkdigitaalerfgoed.nl/wp-content/uploads/2020/12/20210122-Naar-een-geharmoniseerde-meting-van-gebruik-en-impact-van-digitaal-erfgoed-v111.pdf>.

[40] Art. 2 *AR*.

Il sistema è basato modello OAIS[41]: il software di base viene fornito con un'ampia documentazione e consiste fondamentalmente in due parti, ovvero l'applicazione di base e i flussi di lavoro per l'ingest, la gestione dei dati, lo storage e l'accesso. Il software utilizzato è la soluzione di conservazione digitale Preservica, mentre i flussi di lavoro sono mantenuti dal NANETH: alcuni sono predefiniti e vengono forniti con il software e-Depot, altri vengono customizzati per particolari esigenze; in ogni caso, non vengono creati workflow che aggiungono funzionalità completamente nuove, ma la maggior parte esegue ancora la stessa funzione dei flussi standard, ma con modifiche che si adattano meglio all'espandersi dell'infrastruttura. Alcuni modifiche, ad esempio, sono state apportate per controllare i metadati rispetto a specifici schemi XML, o per assicurare che gli oggetti informativi digitalizzati o nativi digitali siano elaborati in modo diverso al momento del versamento, al fine di inoltrare il corretto set di metadati al sistema di gestione delle collezioni.

Per il monitoraggio sul prodotto e-Depot, dopo aver consultato gli *stakeholder*, il *product owner* procede a comunicare le richieste di modifica con il team di sviluppo e il team di gestione delle applicazioni. Per quanto riguarda, invece, gli updates di Preservica, vengono rilasciati uno o due aggiornamenti all'anno: questi sono accompagnati da note e sono solitamente presentati in webinar, che, insieme a un forum di utenti, sono utilizzati per ottenere un *feedback* dagli utenti ai fini dello sviluppo della soluzione[42]. Queste dinamiche forniscono la garanzia di un aggiornamento continuo e basato sull'esperienza degli utenti, nonché le basi per permettere anche un certo margine di previsione per gli sviluppi futuri.

Per lo sviluppo di e-Depot sono impiegati altri strumenti di terze parti, come DROID per il profiling del formato dei file[43] e JHOVE per l'identificazione del formato, la convalida e

[41] Sulla realizzazione e-Depot, si vedano l'*application* per il CoreTrustSeal consultabile al link <https://www.coretrustseal.org/wp-content/uploads/2019/07/e-Depot-of-the-National-Archives-of-the-Netherlands.pdf> e il contributo di Remco van *Veenendaal Preservation impact assessments: how preservation tools support NANETH's connection projects Preservation impact assessments: how preservation tools support NANETH's connection projects*, pubblicato sul blog dell'Open Preservation Foundation il 17 maggio 2017 al link <https://openpreservation.org/blogs/preservation-impact-assessments-how-preservation-tools-support-naneths-connection-projects/>.

[42] Si veda, su Preservica, il capitolo I.3.

[43] DROID (*Digital Record Object Identification*) è uno strumento software gratuito sviluppato dai *National Archives* (UK) finalizzato a profilare automaticamente un'ampia gamma di formati di file: Ad esempio, rileva le versioni, la data, la dimensione e l'ultima modifica, consentendo un'identificazione più precisa dei rischi e la pianificazione di azioni di mitigazione (si veda, in proposito, <http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/file-profiling-tool-droid/>).

la caratterizzazione degli oggetti digitali[44]: entrambi gli strumenti si basano sulle informazioni sul formato dei file fornite dal registro tecnico dell'e-Depot, a sua volta modellato su PRONOM[45]. Esempi di altri *tools* di terze parti utilizzati nell'ambito e-Depot sono le librerie di OpenOffice per la conversione e l'anteprima dei documenti e la libreria *JAI Image I/O Tools* per la conversione dei formati immagine [46].

Per quanto riguarda la sicurezza delle informazioni dell'e-Depot, è utilizzata la National Information Security Baseline[47], insieme a ulteriori misure di sicurezza come audit periodici per lo status dell'intero sistema. Nel luglio 2019, inoltre, l'e-Depot ha ricevuto il *CoreTrustSeal for Trustworthy Data Repositories*[48].

Sin da quando il sistema ha cominciato ad essere operativo, i dipartimenti governativi collegano i loro sistemi informativi all'e-Depot seguendo un procedimento che prevede vari step[49].

I progetti di integrazione sono sempre preceduti da una cosiddetta valutazione d'impatto: esperti di vari dipartimenti NANETH e rappresentanti dell'autorità responsabile (fornitore) indagano quali misure organizzative, di contenuto e tecniche sono necessarie per il collegamento. I risultati di questa valutazione costituiscono gli input per il piano di progetto per stabilire le modalità di assimilazione effettiva.

È importante la considerazione di tali analisi anche come *feedback* per migliorare la strumentazione: viene, infatti, esaminata una selezione rappresentativa degli oggetti informativi dal punto di vista della conservazione, richiedendo informazioni riguardo alle caratteristiche degli oggetti da conservare e all'impatto che queste avranno sul sistema già in essere, al loro eventuale contenuto interattivo o dinamico, alla conformità dei formati

[44] Si veda, su JHOVE, il capitolo I.3.

[45] Si veda, su PRONOM, il capitolo I.3.

[46] <https://www.oracle.com/java/technologies/install-jai-imageio-1-0-01.html>

[47] Lo standard *Baseline Informatiebeveiliging Rijksdiens*t (BIR 2012), basato su ISO 27001 e 27002, è consultabile al link <https://www.nationaleombudsman.nl/system/files/bijlage/BIR_TNK_1_0_definitief.pdf>.

[48] Si veda, in proposito, il capitolo I.3. Riguardo al conseguimento della certificazione per l'e-Depot, si veda <https://www.nationaalarchief.nl/en/archive/knowledge-base/coretrustseal>.

[49] Le istruzioni sono pubblicate sul sito istituzionale dell'Archivio Nazionale al link <https://www.nationaalarchief.nl/archiveren/overbrengen-voor-rijksoverheden>.

utilizzati rispetto al range considerato dal NANETH, alla presenza di oggetti crittografati o firmati e se abbiano già subito conversioni o migrazioni.

Per supportare questa indagine, si utilizzano strumenti per analizzare gli oggetti e i set di dati, proprio per verificare e validare le estensioni e correggere i metadati.

Sono impiegati, in particolare, il *File Information Tool Set* (FITS), sviluppato e curato dall'Università di Harvard, e *Clever, Crafty, Content Profiling of Objects* (c3po), implementato dalla TU Wien.

FITS identifica, convalida ed estrae metadati tecnici su un'ampia gamma di formati di file: agisce come un *wrapper*, richiamando e gestendo l'output da diversi altri strumenti open source[50], C3po è uno strumento software in prototipo, che utilizza i metadati estratti dai file di una raccolta digitale come input per generare un profilo del set di contenuti.

FITS e c3po sono utilizzati attraverso la riga di comando, per creare un profilo c3po per il set di dati rappresentativo. Questo set viene selezionato nell'interfaccia web di c3po, che presenta grafici e altre informazioni in base al profilo, ad esempio quanti file sono presenti nel *dataset*, in quale formato e in quale versione, se sono ben formati e validi, quando sono stati creati e a quando risale l'ultima modifica.

Tuttavia, le informazioni sui formati dei file non comprendono la valutazione dei comportamenti interattivi: i *datasets* costituiti da file di testo e immagini hanno un impatto sul sistema di conservazione più basso, mentre differente è il discorso di database e software.

In ogni caso, vengono preferiti i formati aperti, comuni e ben documentati, rispetto ai formati proprietari e scarsamente utilizzati: viene effettuata l'analisi anche in considerazione del numero di versioni del formato identificato dagli strumenti sopra menzionati. Importante è anche il controllo che siano ben formati e validi: il primo aspetto è collegato alla sintassi, il secondo alla semantica.

Sebbene non per tutte le estensioni, gli strumenti possono fornire informazioni sulla crittografia o sulla protezione tramite password dei file: queste devono essere rimosse prima

[50] Su FITS si veda la pagina dedicata sul sito istituzionale della University of Harvard al link <https://projects.iq.harvard.edu/fits/introduction>.

del versamento in e-Depot: il sistema prevede la gestione degli accessi e la restrizione, ma non la crittografia o la protezione con password sui singoli file.

Per quanto riguarda le date di creazione e modifica, si possono valutare eventuali incoerenze attraverso il confronto tra le informazioni che emergono dalle analisi con FITS e c3po con i metadati dal sistema di origine, in modo da poter disporre del dato corretto.

Le indagini preliminari, unite all'utilizzo degli strumenti FITS, C3po e delle altre soluzioni citate, consentono di disporre dei dati necessari per le valutazioni sugli sviluppi futuri del sistema.

L'integrazione, infine, oltre alla pianificazione del progetto e la valutazione d'impatto, include gli accordi contrattuali, la comunicazione e la gestione delle relazioni. Le misure tecniche, dato che la Legge sugli Archivi prevede che questi siano in buone condizioni, adeguatamente organizzati e accessibili, comprendono anche l'esame del contenuto degli oggetti informativi.

Standard e linee guida

Nell'ambito del *Nationaal Archief* vengono messe a disposizione una serie di risorse sul tema: è presente l'apposita sezione di guida *Preservering* sul sito istituzionale[51] e sono pubblicati l'*Open data collection policy*, la lista dei formati preferiti e accettabili, la *preservation policy*, il catalogo dei prodotti e servizi, il *profile and policy private archives* e il *Netherlands Model Architecture for National Archival Institutions*. A tal proposito, è da menzionare anche l'attività del *Netwerk Digitaal Erfgoed*, ovvero la Rete olandese per il patrimonio digitale: si tratta di una partnership nei Paesi Bassi che si concentra sullo sviluppo di un sistema di strutture e servizi nazionali per migliorare la visibilità, l'usabilità e la sostenibilità del patrimonio digitale; questa rete è aperta a tutte le istituzioni e organizzazioni nel campo del patrimonio digitale[52].

Esiste, inoltre, l'ente nazionale olandese per la standardizzazione, lo *Stichting Koninklijk Nederlands Normalisatie Instituut* (NEN)[53]: questo, organizzato in comitati, collega e

[51] <https://www.nationaalarchief.nl/archiveren/preservering>.
[52] Si veda, in proposito, il sito web al link <www.netwerkdigitaalerfgoed.nl/en>.
[53] Si veda, in proposito, il sito web dell'Istituto reale olandese per la standardizzazione al link <https://www.nen.nl/en/>.

coordina i soggetti coinvolti dall'area trattata dagli standard e dalle linee guida, coprendo un range di oltre NEN gestisce oltre trentunomila standard tra internazionali (ISO, IEC), europei (EN) e nazionali (NEN) accettati nei Paesi Bassi. Saranno annoverati nel nuovo Regolamento sugli archivi gli standard selezionati per l'applicazione alla conservazione a lungo termine.

Per quanto riguarda, invece, le direzioni a riguardo, il *Forum Standaardisatie* mira a facilitare la cooperazione digitale e l'interoperabilità tra organizzazioni governative e tra amministrazione statale, imprese e cittadini[54]. Il Forum contribuisce agli obiettivi di e-government, come il miglioramento dei servizi governativi riducendo le attività eseguite manualmente e automatizzando il flusso di informazioni tra il governo con i cittadini e le imprese: questo corrisponde alla politica olandese di prediligere l'utilizzo di standard aperti per supportare l'interoperabilità, il riuso dei dati e una minore dipendenza da fornitori specifici.

È stato istituito su iniziativa del *Ministerie van Economische Zaken en Klimaat* (Ministero degli Affari economici) nel 2006 per garantire l'attuazione delle strategie sullo scambio elettronico di dati e il riutilizzo di dati e servizi elettronici: fornisce consulenza alla *Overheidsbreed Beleidsoverleg Digitale Overheid* (Consultazione sulla politica del governo digitale) e il suo segretariato fa parte di *Logius*, il servizio di governo digitale del ministero dell'Interno e delle Relazioni del Regno e lo stesso. Sostiene, dunque, il governo olandese nella creazione, nello sviluppo e nell'applicazione di standard aperti per lo scambio di informazioni elettroniche, al fine di prevenire il *vendor lock-in* e ridurre i costi nella spesa governativa per l'ICT. L'attività di questo organismo è volta alla dimensione internazionale: supporta, infatti, l'adozione di standard internazionali, partecipa alla *European Multi-Stakeholder Platform on ICT Standardisation* (MSP)[55] della Commissione Europea e contribuisce alla crescita di ISA², *Interoperability solutions for public administrations, businesses and citizens*[56], il programma della Commissione europea per promuovere soluzioni di interoperabilità per le pubbliche amministrazioni, le imprese e i cittadini.

[54] Si veda, in proposito, il sito web del Forum al link < https://forumstandaardisatie.nl/>.
[55] <https://digital-strategy.ec.europa.eu/en/policies/multi-stakeholder-platform-ict-standardisation>.
[56] <https://ec.europa.eu/isa2/home_en>.

III.5 Romania[1]

III.5.1 Introduzione

In Romania la definizione dei temi relativi agli archivi digitali è attualmente in fase di evoluzione: si sta tentando, attraverso il subentro dell'Autorità per la Digitalizzazione della Romania alle funzioni precedentemente assegnate al Ministero delle Comunicazioni e della Società dell'Informazione, di isolare le competenze digitali nell'ambito di un unico organo, che, tra le varie funzioni, si occupa anche del rilascio dell'autorizzazione a prestare servizi di archiviazione elettronica.

I provvedimenti emanati in materia di documentazione elettronica sono relativi al triennio sono relativi al triennio 2007-2009 e si noteranno, a riguardo, diverse criticità. Sono piuttosto incoerenti dal punto di vista archivistico ed ereditano le carenze della legge archivistica stessa[2]: si osserva un'assenza di riferimenti alle fasi di formazione, gestione e conservazione della documentazione e si lasciano piuttosto indeterminati i confini tra queste attività, in particolare in relazione ai *records* elettronici. La stessa normativa che delimita l'ambito delle autorizzazioni a prestare servizi di 'archiviazione elettronica' lascia indefinito, con questa dicitura, l'oggetto: non si chiarisce se si tratti di gestione o conservazione.

Va rilevata, a riguardo, anche una evidente mancanza di coinvolgimento delle autorità archivistiche e degli Archivi Nazionali sulle questioni inerenti ai documenti e agli archivi digitali: in un primo momento, come si è detto, si è lasciata la facoltà di legiferare in materia all'MCSI, per poi farne confluire le funzioni sull'ADR, ma non si riscontra una presa di consapevolezza, attuata tramite modifiche e integrazione ai dispositivi normativi,

[1] La bibliografia e le risorse telematiche per il contesto rumeno sono state reperite attraverso i contatti con Adrian Dinculescu, Partnerships & Alliances Manager di Namirial S.r.L. Romania e la corrispondenza con l'Autorità rumena per la Digitalizzazione (ADR), tramite richieste protocollate recanti la firma di Sabin-Ioan Sarmas, presidente dell'ADR. Si segnalano, inoltre, i riferimenti dei principali siti web istituzionali consultati: sito web dell' *Autoritatea pentru Digitalizarea României* <https://www.adr.gov.ro/>, ; sito web dell'*Arhivele Naţionale ale României* <http://arhivelenationale.ro/site/>; sezione sull'archiviazione elettronica del sito web del *Ministerul Comunicaţiilor şi Societăţii Informaţionale* <https://www.comunicatii.gov.ro/arhivare-electronica/>.

[2] Posizione, questa, peraltro sostenuta in B-F. Popovici, *Electronic Records Management in Romania: More Electronic-, Less Records-Management*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 183-192 < https://journal.almamater.si/index.php/Atlanti/article/view/126/113>. Per ulteriori approfondimenti, si veda il capitolo IV.2.

dell'importanza del definire dei requisiti diversificati per sistemi di gestione documentale e di conservazione e di adeguarsi, inoltre, alle innovazioni tecnologiche.

III.5.2 Conservazione digitale e contesto amministrativo: organismi preposti al coordinamento delle politiche sugli archivi

L'ambito della gestione e conservazione degli archivi, in Romania, rientra, da un lato, nelle competenze degli *Arhivele Naționale ale României* (Archivi Nazionali della Romania), dall'altro tra quelle dell'*Autoritatea pentru Digitalizarea României* (ADR – Autorità per la Digitalizzazione della Romania).

Arhivele Naționale ale României

Gli Archivi Nazionali sono organizzati e funzionano come un organo specializzato della pubblica amministrazione centrale subordinato al Ministero degli Affari interni[3], che si occupa di gestire le risorse finanziarie destinate a questo ambito e sovrintende la nomina del direttore dell'Archivio Nazionale, il quale coordina le attività delle quarantadue sedi regionali[4]. Questi hanno il compito di amministrare e proteggere il *Fondului Arhivistic Național al României* (Fondo Archivistico Nazionale della Romania), ovvero l'insieme dei

[3] *Lege 16/1996 privind Arhivelor Naționale,* Art. 3, (1) L'amministrazione, la supervisione e la protezione speciale del Fondo archivistico nazionale della Romania sono svolte dagli Archivi Nazionali, che sono istituiti con decisione del governo; a livello di gestione, sono subordinati al Ministero degli affari interni, esercitano le proprie attribuzioni tramite i propri dipartimenti specializzati e tramite i servizi provinciali degli Archivi Nazionali.

[4] Le vicende storiche che hanno interessato il dominio del territorio rumeno e della sua amministrazione hanno determinato l'istituzione del primo archivio di stato nel 1861, a seguito dell'annessione della Valacchia e della Moldavia alla giurisdizione della Romania. Nel 1862, con la formazione ufficiale dello Stato, il governo raccoglie gli archivi dai monasteri, dalla Valacchia e dalla Moldavia e li deposita a Bucharest, sotto l'autorità del Ministero della Giustizia, degli Affari Religiosi e della Pubblica istruzione. Dopo la Prima guerra mondiale, nuove acquisizioni territoriali comportano l'istituzione di nuove sedi degli archivi nazionali in Transilvania, Bucovina e Bessarabia. Nel 1925 viene sancita la creazione degli archivi regionali sotto la tutela del Ministero della Pubblica istruzione e l'obbligo, per gli enti governativi, di consegnare la propria documentazione nell'Archivio di Stato di Bucharest. Nel 1951, con l'inclusione della Romania nell'Unione Sovietica, gli archivi passano sotto il controllo del Ministro degli Affari interni e, al termine del decennio, viene concepito il Fondo Archivistico Nazionale. Nel 1996 la legge sugli Archivi Nazionali sostituisce il titolo Archivio di Stato con Archivio Nazionale della Romania e vincola gli enti pubblici (eccetto il Ministero della Difesa, il Ministero degli Affari esteri, il Servizio rumeno di Intelligence, il Servizio estero di Intelligence e il Servizio di guardia e gli uffici coinvolti in attività di sicurezza nazionale) e privati e le organizzazioni al versamento della documentazione prodotta da venti a cento anni. Gli scopi di questo istituto sono selezionare, raccogliere, gestire e rendere accessibili le testimonianze documentali rilevanti per la memoria e l'identità nazionale; creare e sviluppare *policies* che seguano le leggi rumene; provvedere alla sicurezza e alla protezione del materiale archivistico custodito (Franks, Bernier (a cura di), *The international directory of national archives*, cit., pp. 309-311).

documenti ufficiali e privati, diplomatici e consolari, memorie, manoscritti, proclami, citazioni, manifesti, piani, schizzi, mappe, film cinematografici e altri tali testimonianze, matrici di sigilli, nonché registrazioni di foto, video, audio e digitali con valore storico, realizzate nel paese stesso o da soggetti produttori rumeni che operano all'estero[5].

La stessa Legge sugli Archivi Nazionali che gli attribuisce queste funzioni gli conferisce le ulteriori competenze di elaborare norme e metodologie di lavoro per l'organizzazione e lo sviluppo dell'attività archivistica, anche per la classificazione e l'inclusione nel Fondo Archivistico Nazionale della Romania dei documenti sopra menzionati e di controllarne l'applicazione, di subentrare ai soggetti produttori nella custodia dei documenti che fanno parte del Fondo Nazionale Archivistico della Romania, e di assicurarne l'inventario, la selezione, l'archiviazione e la fruibilità. Di istituire e sviluppare la banca dati degli Archivi Nazionali il relativo sistema informativo, di stabilire misure per la correlazione tecnica e metodologica e per la collaborazione dei servizi di informazione e documentazione archivistica e dipartimenti analoghi all'interno del Sistema nazionale di informazione e documentazione[6].

In relazione allo sviluppo e all'utilizzo delle tecnologie in ambito archivistico, però, il legislatore ha optato per la delega delle questioni relative alla digitalizzazione degli archivi e ai documenti informatici al Ministero delle Comunicazioni e della Società dell'Informazione, cui è subentrata, nel gennaio 2020, l'Autorità per la Digitalizzazione della Romania.

***Autoritatea pentru Digitalizarea României* (ADR)**

L'ente che in Romania si occupa della gestione delle pratiche inerenti alla gestione e alla conservazione degli archivi elettronici è l'Autorità per la Digitalizzazione della Romania), organizzazione sotto il diretto controllo del Primo Ministro rumeno. Questo organismo è di recentissima costituzione ed è succeduto, in base a quanto stabilito nella Decisione n. 89 del 10 gennaio 2020 sull'organizzazione e il funzionamento dell'Autorità rumena per la

[5] Art. 2 Lege 16/1996 *privind Arhivelor Naționale,*.
[6] Art. 5 Lege *16/1996*,.

Digitalizzazione[7], al *Ministerul Comunicaţiilor şi Societăţii Informaţionale* (MCSI – Ministero delle Comunicazioni e della Società dell'informazioni)[8] nell'ambito dell'archiviazione digitale, delle comunicazioni elettroniche e delle tecnologie dell'informazione. Questa stessa Decisione, oltre a rappresentarne l'atto costitutivo, descrive i compiti dell'ADR: questa è incaricata di elaborare le strategie di pianificazione per le politiche di trasformazione digitale e il quadro normativo, metodologico e funzionale per l'adozione e l'attuazione di tali decisioni, emanando linee guida autonome o di concerto con le altre entità pertinenti, con particolare attenzione al recepimento della legislazione europea in materia di società dell'informazione, tecnologia e interoperabilità dei sistemi. A tal proposito, rappresenta anche l'autorità statale che assicura la vigilanza e il controllo sull'osservanza di tutti i provvedimenti nel proprio ambito di competenza.

Dunque, per quanto riguarda gli aspetti specificatamente connessi alla conservazione digitale, si occupa, innanzitutto, del procedimento di autorizzazione degli amministratori di archivi digitali[9] e dei data center, al fine di redigere, aggiornare e pubblicare sul proprio sito istituzionale elenchi che contengono le denominazioni dei prestatori di servizi fiduciari e le informazioni sulla tipologia dei servizi offerti. Esercita, dunque, i poteri di organo di vigilanza e controllo su tali fornitori con sede legale in Romania e adotta misure alternative di audit nel caso di incarichi affidati ad aziende di altri Paesi europei, in conformità a quanto stabilito dal regolamento eIDAS. Inoltre, relativamente al contenuto degli archivi digitali, l'ADR ha accesso ai documenti, ai dati o informazioni[10], indipendentemente dalla loro forma e dall'ambiente o dal luogo in cui sono conservati: può, infatti, imporre a qualsiasi persona fisica o giuridica, pubblica o privata, l'obbligo di renderli disponibili, al fine di determinare eventuali violazioni e intraprendere eventuali azioni sanzionatorie.

[7] Hotărâre nr. 89 din 28 ianuarie *2020 privind organizarea şi funcţionarea Autorităţii pentru Digitalizarea României*.

[8] Le informazioni riguardo la struttura e il funzionamento del Ministero delle Comunicazioni e della Società dell'Informazione rumeno sono consultabili sul sito istituzionale <https://www.comunicatii.gov.ro/>.

[9] È così definita nell'art. 5 comma 1 dell'Ord. 493/2009 (si veda il paragrafo III.5.3) «la persona fisica che ha il ruolo di supervisione e attuazione delle attività di gestione di un archivio elettronico per terzi, o la persona giuridica che ha il ruolo di supervisione e attuazione dell'attività di gestione di un archivio elettronico a proprio nome o per terzi ed è responsabile della gestione del sistema di archiviazione elettronica e dei documenti archiviati elettronicamente».

[10] Queste facoltà sono attribuite attraverso l'applicazione del Regolamento UE 2017/2394 sulla cooperazione tra autorità nazionali, in rispetto a quanto previsto in materia di protezione di dati personali.

III.5.3 Disposizioni sulla conservazione dei documenti e degli archivi digitali

Il tracciamento dei provvedimenti normativi in materia di conservazione digitale è composito, sebbene relativamente poco complesso, in quanto la legislazione relativa all'archiviazione elettronica dei documenti è circoscritta a un numero limitato di provvedimenti.

Lege privind Arhivelor Naționale* e *Lege privind arhivarea documentelor în formă electronică

In primo luogo, il riferimento principale per la conservazione degli archivi pubblici è la Legge del 2 aprile 1996 sugli Archivi Nazionali[11], ripubblicata nel 2014 a seguito degli ultimi aggiornamenti apportati dalla Legge n. 138/2013 per la modifica e il completamento della Legge sugli Archivi Nazionali[12].

Secondo le disposizioni di questa legge, le persone fisiche e giuridiche che producono i documenti che sono considerabili come parte del Fondo Archivistico Nazionale della Romania[13] sono responsabili della loro gestione e della loro conservazione[14], mentre gli Archivi Nazionali forniscono assistenza specializzata, assicurano il coordinamento e l'adozione di regole archivistiche uniformi per i titolari dei documenti stessi e subentrano nella custodia di tale documentazione ai fini di preservarne la memoria storica[15].

In particolare, per quanto riguarda la conservazione dei documenti, i soggetti produttori e i titolari dei documenti sono tenuti a conservare i documenti in condizioni adeguate, assicurandoli da distruzione, deterioramento, appropriazione indebita o commercializzazione in condizioni diverse da quelle previste dalla legge, sino a che non risultano destinati alla

[11] Lege nr. 16 din 2 aprilie 1996 *privind Arhivelor Naționale*.

[12] Lege nr. 138 din 30 aprilie 2013 *pentru modificarea și completarea Legii Arhivelor Naționale nr. 16/1996, publicată în Monitorul Oficial al României, Partea I, nr. 253 din 7 mai 2013*. È da menzionare che, dal primo agosto 2017, risulta in consultazione il progetto di legge archivistica (*Lege Archivelor,* visionabile al link <http://arhivelenationale.ro/site/download/acte_normative/Proiectul-Legii-Arhivelor.pdf> - ultima consultazione: 18/02/2021): questa raccoglie le disposizioni della legge sugli Archivi Nazionali, le completa e le integra con dettagli relativi alla documentazione e agli archivi elettronici.

[13] Art. 2, *Lege nr. 16/1996*; si veda, in proposito, il paragrafo III.5.2.

[14] Art. 4, *Lege nr. 16/1996*. È stato emanato, in ottemperanza a queste disposizioni, il documento *Instrucţiuni privind activitatea de arhivă la creatorii şi deţinătorii de documente, aprobate de conducerea Arhivelor Naţionale prin Ordinul de zi nr. 217 din 23 mai 1996* (Istruzioni sulle attività di archiviazione per soggetti produttori e titolari di documenti).

[15] Art. 5, *Lege nr. 16/1996;* si veda, in proposito, il paragrafo III.5.2.

conservazione permanente. I documenti che si prevede vengano versati a questo scopo presso Archivi Nazionali e presso i servizi della contea degli Archivi nazionali sono i documenti fotografici e film dopo 20 anni dalla loro creazione, i documenti scritti, ad eccezione degli atti di stato civile e documenti tecnici, dopo 30 anni dalla loro creazione, i documenti tecnici dopo 50 anni dalla loro creazione, i documenti di stato civile dopo 100 anni[16].

La Legge archivistica consente che operatori economici possano fornire servizi per la conservazione di documenti e archivi, ma disciplina soltanto il caso in cui essi siano analogici[17].

Nel 2007[18] queste disposizioni, che, per lo più, non tangono gli aspetti relativi ai documenti e agli archivi digitali, sono state integrate con un dispositivo specifico che delimita in maniera circoscritta l'ambito dell'archiviazione digitale, la Legge n. 135 del 15 maggio 2007 in materia di archiviazione dei documenti in formato elettronico[19]. Questa definisce il regime legale applicabile alla creazione, conservazione, consultazione e utilizzo di documenti in formato elettronico, in conformità con quanto indicato dalle disposizioni della

[16] Art. 13, *Lege nr. 16/1996.* L'art. 14 specifica che i produttori e titolari dell'archivio possono detenere documenti che fanno parte del Fondo Nazionale Archivistico della Romania anche dopo la scadenza del termine di presentazione, se necessari allo svolgimento della loro attività, previa approvazione del direttore degli Archivi Nazionali, nel caso degli uffici centrali. Anche il Ministero della Difesa Nazionale, il Ministero degli Affari Esteri, il Servizio di intelligence rumeno, il Servizio di intelligence estero, il Servizio di sicurezza e l'Accademia rumena conservano i propri documenti a queste condizioni. Sono però tenuti, in base all'art. 17, a presentare agli Archivi Nazionali o ai servizi provinciali degli Archivi Nazionali, a seconda dei casi, copia degli inventari dei documenti permanenti in loro possesso allo scadere dei termini per la loro presentazione.

[17] Art. 19 *Lege nr. 16/1996.* Gli operatori economici possono fornire servizi per l'archiviazione, la conservazione, il restauro, la rilegatura, il trattamento archivistico e l'uso di documenti di valore corrente in loro possesso, di seguito denominati servizi di archiviazione, solo dopo aver ottenuto la licenza di esercizio dagli Archivi Nazionali, dai servizi della contea o dal Servizio municipale di Bucarest degli archivi nazionali, a seconda dei casi. L'autorizzazione operativa viene rilasciata, a pagamento, secondo le disposizioni di legge, per uno o più servizi di archiviazione, sulla base delle competenze professionali del personale impiegato, delle risorse materiali di cui l'operatore dispone e sui regolamenti archivistici interni di gestione. Questa autorizzazione viene rilasciata per un periodo di 3 anni e può essere rinnovata per lo stesso periodo: per il rinnovo dell'autorizzazione di esercizio, l'operatore deve presentare agli Archivi Nazionali, ai servizi della contea o al servizio municipale di Bucarest degli Archivi Nazionali, a seconda dei casi, la documentazione aggiornata comprovante l'adempimento delle condizioni iniziali di acquisizione. I contratti per la fornitura di servizi di archiviazione devono contenere clausole espresse relative al trasferimento di documenti presi in carico dall'operatore economico autorizzato a fornire servizi di archiviazione, in caso di cessazione della sua attività, ad un altro operatore economico autorizzato a fornire servizi di archiviazione (Art. 22). Gli Archivi Nazionali garantiscono il registro generale degli operatori economici autorizzati a fornire servizi di archiviazione, attraverso il Registro degli operatori economici che forniscono servizi di archiviazione (Art. 25).

[18] Si noti che il primo gennaio 2007 la Romania diviene Paese membro dell'Unione Europea, circostanza che ha portato la Romania ad adeguarsi alle spinte di digitalizzazione (<https://europa.eu/european-union/about-eu/countries/member-countries/romania_it>).

[19] Lege nr. 135 din 15 mai 2007 *privind arhivarea documentelor în formă electronică*.

Legge sugli Archivi Nazionali n. 16/1996 e dalle norme vigenti in materia di conservazione, accesso e protezione delle informazioni di natura pubblica o privata[20].

Il versamento di un documento informatico in un archivio elettronico, secondo provvedimento, può essere effettuato se è sottoscritto elettronicamente, con firma valida, dal titolare del diritto di disposizione sul documento, se viene trasmesso con i metadati indicati dall'articolo 8[21] e se, in caso siano documenti crittografati, le chiavi vengono depositate agli Archivi Nazionali[22].

Dunque, l'amministratore dell'archivio elettronico firma elettronicamente i documenti in ingresso, attestando che il documento ha il valore di originale o copia a seconda della decisione del titolare del diritto di disposizione sul documento e ha il compito di conservare, insieme al documento elettronico archiviato, il file contenente i metadati sopra menzionati. Il documento in forma elettronica, così identificato, è archiviato ove stabilito dall'amministratore dell'archivio elettronico[23], che è tenuto a conservare anche un record dei documenti elettronici inseriti nel sistema di archiviazione sotto forma di registro, a sua volta elettronico[24].

---

[20] Artt. 1-2, *Lege nr. 135/2007*.

[21] *Lege 135/2007* Art. 8 (2) L'amministratore dell'archivio elettronico allega, per ogni documento in formato elettronico archiviato, un file in formato elettronico che conterrà almeno le seguenti informazioni: a) il proprietario del documento in formato elettronico; b) l'emittente del documento in formato elettronico; c) il titolare del diritto di disposizione sul documento; d) la storia del documento in formato elettronico; e) il tipo di documento in formato elettronico; f) il livello di classificazione del documento in formato elettronico; g) il formato digitale in cui il documento è archiviato in formato elettronico; h) le parole chiave necessarie per identificare il documento in forma elettronica; i) gli elementi per individuare il supporto fisico; j) l'identificativo univoco del documento in formato elettronico all'interno dell'archivio elettronico; k) la data di rilascio del documento; l) data di archiviazione; m) il termine di conservazione del documento.

(3) Se il documento in formato elettronico è stato generato trasferendo le informazioni dai media analogici ai media digitali, la registrazione deve contenere inoltre le seguenti informazioni: a) riferimenti al proprietario dell'originale e al luogo in cui si trova l'originale; b) il metodo di trasferimento utilizzato; c) il dispositivo hardware utilizzato; d) il programma informatico utilizzato.

[22] Art. 7, *Lege nr. 135/2007*.

[23] Art. 8, *Lege nr. 135/2007*.

[24] Art. 9, *Lege nr. 135/2007*. Questo articolo determina anche il regime di accesso al registro dei documenti: è pubblico solo per i documenti per i quali il titolare del diritto di disposizione sul documento ha istituito un regime di accesso pubblico, mentre il riferimento a un documento appartenente alla categoria dei classificati può essere ottenuto in base ai diritti di accesso del richiedente. A tal proposito, le modalità di consultazione e visibilità dei singoli documenti vengono definite dagli articoli 14 e 15: il regime di accesso a un documento in forma elettronica, nonché la sua modifica, sono stabiliti esclusivamente dal titolare del diritto di disposizione sul documento mediante un atto firmato sia dal titolare del diritto di disposizione sul documento sia dall'amministratore archivio elettronico; le condizioni di accessibilità del documento sono inserite nel file elettronico del documento e il documento che istituisce queste regole, generato elettronicamente o trasferito in formato elettronico, costituirà un allegato al documento archiviato. L'amministratore dell'archivio elettronico

Autorizzazioni dell'amministratore di archivio elettronico e del data center

Vi sono, poi, delle ordinanze rivolte al conseguimento dell'autorizzazione per poter fornire servizi di archiviazione elettronica, che riguardano l'accreditamento dell'amministratore degli archivi elettronici e il data center che ospita i dati e ne consente la gestione. Il primo ambito è anticipato nella legge 2007, che all'art. 3 definisce come amministratore dell'archivio elettronico la persona fisica o giuridica accreditata dall'autorità di regolamentazione e di vigilanza specializzata nel settore per amministrare il sistema di archiviazione elettronica e i documenti archiviati all'interno di questo deposito elettronico; questo, innanzitutto, deve disporre di risorse finanziarie per coprire i danni che potrebbero essere recati durante lo svolgimento delle attività di archiviazione elettronica, con modalità assicurativa stabilita dall'autorità di regolamentazione e di vigilanza, e, nel caso debba contenere documenti classificati, deve soddisfare le condizioni legali relative alla protezione delle informazioni classificate[25].

L'autorizzazione a ricoprire il ruolo di amministratore di archivio elettronico è vincolata dall'Ordinanza del MCSI n. 493 del 15 giugno 2009 sulle norme tecniche e metodologiche per l'applicazione della Legge n. 135/2007 in materia di archiviazione dei documenti in formato elettronico[26], che, in conformità con quest'ultima, stabilisce la procedura per la concessione, la sospensione o la revoca dell'accreditamento degli amministratori degli archivi elettronici e le condizioni per lo svolgimento di tale attività[27]. Il provvedimento conferiva la responsabilità della regolamentazione, della verifica e della vigilanza al Ministero delle Comunicazioni e della Società dell'Informazione, ma, da gennaio 2020, queste competenze sono state assegnate all'ADR[28].

è tenuto a rispettare queste condizioni sia per l'archiviazione sia per la concessione dell'accesso al documento; la responsabilità di stabilire il regime di accesso riguarda esclusivamente il titolare del diritto di disposizione sul documento, mentre la responsabilità del rispetto di tale regime spetta all'amministratore dell'archivio elettronico, che garantisce le modalità di consultazione permanente o su richiesta per ciascun documento.

[25] Art. 10, *Lege nr. 135/2007*.

[26] *Ordin nr. 493 din 15 iunie 2009 privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică*.

[27] Art. 1, *OMCSI nr. 493/2009*. L'elenco degli amministratori di archivio elettronico autorizzati (in numero di 27 all'ultima consultazione del 20/11/2021) è pubblicato e aggiornato dall'ADR sul proprio sito istituzionale al link <https://www.adr.gov.ro/arhivare-electronica/>.

[28] Si veda, in proposito, il paragrafo III.5.2.

In primo luogo, viene specificato che l'amministratore è la persona fisica o giuridica che ha il ruolo di supervisione e attuazione dell'attività di gestione di un archivio elettronico a proprio nome o per terzi ed è responsabile della gestione del sistema di archiviazione elettronica e dei documenti archiviati elettronicamente e che chi intende ottenere tale qualifica ha l'obbligo di inviare all'ADR una notifica trenta giorni prima di cominciare l'attività. Questa richiesta deve essere corredata dalla documentazione che attesti le qualifiche del personale impiegato dall'amministratore, che dimostri la rispondenza a determinati requisiti funzionali e di sicurezza e che contenga i dati identificativi del data center che ospita l'archivio elettronico, dalla descrizione di politica e procedure relative alla sicurezza e alla conservazione dei dati (compresa la protezione dei dati personali) e, nel caso il richiedente intenda fornire servizi di archiviazione elettronica a terzi, da una lettera di garanzia di un istituto finanziario specializzato o una polizza assicurativa di responsabilità civile almeno pari all'equivalente in lei dell'importo di 300.000 euro, con cui coprire i danni che potrebbero essere causati nello svolgimento di attività di archiviazione elettronica[29].

Per quanto riguarda la gestione dell'archivio elettronico, viene chiarito che è regolata dalle stesse modalità previste per i documenti cartacei ed è soggetta alle disposizioni della legislazione archivistica in vigore: la registrazione dei documenti in formato elettronico (completa del file di metadatazione) da parte del sistema di archiviazione elettronica certifica l'esistenza ufficiale dei rispettivi documenti; il numero di registrazione identifica in modo univoco il documento all'interno del sistema e, una volta registrato, il documento non potrà

[29] Art. 5, *OMCSI nr. 493/2009*, come da modifiche a seguito del subentro dell'ADR alle funzioni dell'MCSI. Nello specifico, la notifica va compilata seguendo il modello proposto nell'allegato n. 2 del provvedimento stesso. Per quanto riguarda le qualifiche del personale, si richiedono: a) certificazioni per la persona fisica o per i dipendenti della persona giuridica che intende diventare amministratore o della persona giuridica subappaltata a tale scopo (le certificazioni possono essere cumulativamente detenute da più dipendenti della persona giuridica), che consistono in: diploma di laurea di studi superiori nel campo dell'informatica; qualifiche o certificazioni che confermano la conoscenza delle norme ISO IEC 27001 o standard equivalenti e delle loro versioni successive, nel campo della gestione di database e dei sistemi operativi e in ambito archivistico; b) documenti che dimostrano che il sistema di archiviazione elettronica garantisca i mezzi di controllo e sicurezza dei documenti e della banca dati; mantenga l'integrità interna, il funzionamento e la coerenza del sistema e della banca dati; assicuri la conservazione illimitata dei documenti di carattere permanente e l'eliminazione definitiva di coloro che hanno un termine di conservazione scaduto, secondo la nomenclatura archivistica, salvo nei casi previsti dalla legge; assicuri i processi di inserimento dei documenti nel sistema amministrativo; assicuri la funzione di ricerca dei documenti; garantisca l'accesso ai documenti archiviati, in conformità con il regime di accesso stabilito, nonché la possibilità di utilizzare i documenti; assicuri le funzioni di amministrazione e cancellazione dei documenti, garantendo il controllo delle operazioni al fine di eliminare il rischio di accesso non autorizzato ai documenti e di distruzione inappropriata dei documenti;

più subire modifiche di contenuto. Il sistema di archiviazione dei documenti deve generare automaticamente un "record di evidenza", in cui sono registrate, senza possibilità di modifica, tutte le modifiche e le azioni che si verificano su un documento dal momento della registrazione e fino alla sua distruzione o trasferimento agli Archivi Nazionali[30].

Gli amministratori che forniscono servizi di archiviazione elettronica a terzi hanno l'obbligo di rendere pubbliche, attraverso il proprio sito web i dati di contatto dell'amministratore, la descrizione generale delle politiche, procedure e tecnologie utilizzate nell'attività di archiviazione elettronica, le limitazioni al diritto di accesso ai documenti archiviati, gli obblighi dei soggetti beneficiari e la disponibilità di servizi[31].

La stessa Ordinanza 493/2009, inoltre, specifica anche le condizioni per il soggetto beneficiario del servizio che versa i documenti nell'archivio elettronico: al fine di depositare un documento nell'archivio elettronico, è necessario soddisfi le condizioni stabilite dalle disposizioni della Legge n. 135/2007[32], che possegga un certificato digitale qualificato per la firma elettronica in corso di validità e che comunichi all'amministratore le informazioni necessarie per verificare la validità del certificato utilizzato per la firma elettronica dei documenti archiviati nell'archivio elettronico. Il beneficiario, d'altro canto, ha il diritto di stabilire il regime di accesso al documento archiviato e di modificarlo, di attestazione del valore dell'originale o della copia del documento archiviato, di accesso online alla documentazione elettronica e al file elettronico obbligatorio di metadati allegato a ciascun documento inserito nell'archivio elettronico, secondo il regime di consultabilità stabilito e di accesso ai programmi utilizzati dall'amministratore nell'attività di archiviazione, necessari per l'accesso ai documenti personali che sono stati archiviati[33].

Per quanto riguarda, invece, l'autorizzazione dei data center utilizzati dagli amministratori di archivi elettronici, questa è normata dall'Ordinanza del MCSI n. 489 del

[30] Art. 12, *OMCSI nr. 493/2009*. Lo stesso articolo prevede che nel caso in cui i documenti siano trasferiti dal sistema, rispettivamente migrati dal supporto iniziale, l'evidenza dei documenti sui nuovi supporti includerà l'evidenza dei supporti esterni e l'evidenza del contenuto dei documenti inclusi. I documenti con lo stesso periodo di conservazione verranno raggruppati su un supporto esterno. i documenti e gli archivi in formato elettronico saranno inseriti nella nomenclatura archivistica dell'organizzazione, specificando nella colonna "Osservazioni", la dicitura "in formato elettronico".

[31] Art. 15, OMCSI nr. 493/2009.

[32] Art. 7, Legge 135/2007 (*v. supra*).

[33] Art. 16, OMCSI nr. 493/2009.

15 giugno 2009 sulle norme metodologiche per l'autorizzazione dei data center[34] e dalle sue successive modificazioni[35]. In queste disposizioni, in conformità con la Legge n. 135/2007, viene stabilito che il data center deve risultare autorizzato dall'ADR, al quale è necessario indirizzare una richiesta scritta[36]. L'ADR verifica il rispetto delle condizioni per l'autorizzazione: nel corso dello svolgimento della procedura, questo organismo può richiedere qualsiasi documento relativo all'attività del data center correlato all'attività di archiviazione elettronica e può svolgere azioni di controllo per accertare la veridicità delle informazioni dichiarate[37].

L'ADR imposta la procedura nominando un revisore designato, selezionato attraverso un processo di qualifica basato sui criteri stabiliti dall'autorità e previa sua selezione tra i candidati abilitati a compiere tale operazione di valutazione. A tale scopo, dopo aver messo a disposizione di qualsiasi parte interessata (su corrispettivo economico) le condizioni per candidarsi al ruolo di auditor, l'autorità rende pubblico l'avviso di selezione, comprensivo del termine per la presentazione della domanda. L'ADR, dunque, verifica i documenti di qualificazione dei candidati e il rispetto dei criteri stabiliti ed entro trenta giorni dalla data di ricevimento della domanda di avvio dell'iter autorizzativo redige e comunica l'elenco di questi ultimi al richiedente l'autorizzazione del data center. Questo, a sua volta, seleziona tra i potenziali revisori quello che sarà nominato dall'autorità con provvedimento pubblico per eseguire le procedure di verifica e valutazione.

Nel corso dell'audit, eseguito a spese del richiedente l'autorizzazione, l'ADR può esaminare ulteriori eventuali documenti relativi alla sua attività e designare il proprio personale per partecipare al processo di audit. Il risultato di queste verifiche viene presentato

[34] *Ordin nr. 489 din 15 iunie 2009 privind normele metodologice de autorizare a centrelor de date*.

[35] Ordine n. 585 del 9 maggio 2011 per completare l'Ordine del Ministro delle comunicazioni e della società dell'informazione n. 489/2009 sulle norme metodologiche per l'autorizzazione dei data center (*Ordin nr. 585 din 9 mai 2011 pentru completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date*) e Ordine 1167 del 25 novembre 2011 per la modifica dell'allegato n. 3 all'Ordine del Ministro delle comunicazioni e della società dell'informazione n. 489/2009 sulle norme metodologiche per l'autorizzazione dei data center (*Ordin nr. 1167 din 25 noiembrie 2011 pentru modificarea Anexei nr. 3 la Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date*).

[36] Art. 4, *OMCSI nr. 489/2009*. La norma fa riferimento al MCSI: come si è già affermato, le competenze di quest'ultimo in materia di archivi elettronici sono state attribuite all'ADR, pertanto, da qui innanzi, il riferimento al MSCI nella normativa viene sostituito con ADR.

[37] Art. 5, *OMCSI nr. 489/2009*.

dal valutatore sotto forma di rapporto di audit, corredato dall'esito di quest'ultimo: l'ADR, a seguito dell'analisi di questa relazione, può accogliere la domanda, rimandarla con riserva (comunicando le difformità sia al revisore sia al richiedente l'autorizzazione) o riservarsi il diritto di respingerla[38].

Per quanto riguarda i requisiti stabiliti dall'Ordinanza per poter superare con successo la procedura, il data center deve garantire la sicurezza e l'integrità dei dati, a livello di sicurezza fisica e informatica: il luogo in cui è collocato il data center deve essere dotato della opportuna aereazione, attrezzato per la prevenzione di incendi e guasti, mentre, dal punto di vista informatico, deve essere efficacemente provvisto di firewall, antivirus, log di tracciamento e controllo dei diritti di accesso. È necessario assicurare la continuità del servizio di archiviazione, attivando procedure di backup delle informazioni e adottando una struttura scalabile[39].

Inoltre, il funzionamento del data center deve essere eseguito nel rispetto di strategie, politiche e procedure ben definite in materia di gestione, controllo e sicurezza dei sistemi, che includano il tracciamento cronologico delle azioni svolte nel sistema (accesso fisico alle apparecchiature, processi di manutenzione, azioni degli operatori, ecc.), monitoraggio a intervalli regolari dell'infrastruttura del data center, del sistema di sicurezza e delle apparecchiature informatiche utilizzate, compresi i sistemi di backup, utilizzo di un sistema di controllo qualità, valutazione degli effetti di estensioni e aggiornamenti, la revisione periodica del piano di sicurezza e l'impiego di personale specializzato con adeguate certificazioni[40].

L'autorizzazione è valida per un periodo di tre anni dalla data della sua emissione: al termine, può essere rinnovata attraverso la medesima procedura effettuata per il primo rilascio. Nel corso della validità dell'autorizzazione, l'ADR ha il diritto di eseguire

[38] Artt. 1, 3-9 *OMCS nr. 585/2011*. L'Ordinanza 585/2011 aggiunge l'allegato 3 all'Ordinanza 489/2009, contenente la descrizione della procedura di autorizzazione. Gli artt. 10 e 11 specificano che, per i casi in cui il data center si trovi al di fuori del Paese, l'audit del sistema viene eseguito dall'auditor rumeno dall'estero o dal revisore rumeno, che si impegnerà a far controllare il sistema da personale qualificato simile proveniente da tale paese o che baserà il proprio certificato su documenti e certificati emessi nel paese in cui il sistema è in esecuzione e che dispongono di un adeguato grado di assicurazione. In ogni caso, tutta la documentazione relativa alla procedura di autorizzazione va redatta in lingua rumena.

[39] Artt. 6-11, *OMCSI nr. 489/2009*.

[40] Art. 12 *OMCSI nr. 489/2009*.

periodiche azioni di controllo, al fine di verificare il mantenimento delle condizioni operative del data center[41].

III.5.4 Modelli e standard di conservazione

Non vi sono, nel contesto rumeno, particolari menzioni di standard legati alla conservazione digitale. Soltanto nell'Ordinanza n. 489/2009, all'articolo 16, viene consigliata per il corretto funzionamento dei data center l'applicazione degli standard ISO/IEC connessi alla sicurezza informatica, tra cui ISO 27001[42].

[41] Art. 14 *OMCSI nr. 489/2009*.

[42] L'art. 16 *dell'OMCSI nr. 493/2009* cita, nello specifico: a) ISO/IEC 17799: 2006 Tecnologia informatica – Tecniche di sicurezza — Codice di buone pratiche per la gestione della sicurezza delle informazioni (ritirato e attualmente sostituito da ISO/IEC 27002:2013 *Information technology – Security techniques – Code of practice for information security controls*; b) *ISO/IEC 27001: 2006 Tecnologia informatica – Tecniche di sicurezza. Sistemi di gestione della sicurezza delle informazioni. Requisiti* (attualmente nella sua versione ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements*); c) ISO/IEC 15408-1:2005 Tecnologia informatica. Tecniche di sicurezza. Criteri di valutazione per la sicurezza della tecnologia dell'informazione. Parte 1: Introduzione e modello generale (ritirato e attualmente sostituito da ISO/IEC 15408-1:2009 *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*); d) ISO/IEC 20000-1: 2005 Tecnologia informatica – Gestione della sicurezza – Parte 1: Specifiche (attualmente sostituito da ISO/IEC 20000-1:2018 *Information technology – Service management – Part 1: Service management system requirements*); e) ISO/IEC 20000-2: 2005 Informatica – Gestione della sicurezza - Parte 2: Codice di condotta (ritirato); f) norma TIA/EIA 942 2005 relativa all'infrastruttura di telecomunicazione del Data Center; g) SR EN 50173-5 2008 Tecnologia informatica. Sistemi di cablaggio generici. Parte 5: Data center (attualmente CEI EN 50173-5 Tecnologia dell'informazione - Sistemi di cablaggio strutturato. Parte 5: Centri di elaborazione dati); h) SR EN 50173-1 2008 Tecnologia dell'informazione. Sistemi di cablaggio generici. Parte 1: Requisiti generali (attualmente CEI EN 50173-1 Tecnologia dell'informazione - Sistemi di cablaggio strutturato. Parte 1: Requisiti generali).

Parte IV. Analisi critica e comparativa

IV.1 Considerazioni generali

La nuova normativa italiana in materia di conservazione digitale

L'Italia possiede un apparato di leggi, provvedimenti e regolamentazioni tecniche sulla conservazione di documenti e archivi digitali ampio e articolato, soggetto di recente a numerose modifiche.

Dalla disamina dei testi, come già affermato, si nota rispetto all'analogico un progressivo distanziamento delle autorità competenti in materia di tutela e valorizzazione dei Beni Culturali dall'ambito decisionale a livello normativo: se nella Legge archivistica del 1963[1] e nel Codice dei Beni culturali[2] si nota una preponderanza sia dispositiva sia operativa delle autorità archivistiche, nel contesto digitale – con il CAD, le Regole Tecniche e le Linee guida – attualmente gli oneri risultano spostati sugli organi competenti in materia di digitalizzazione della Pubblica amministrazione.

Questo implica da un lato l'elaborazione di norme rispondenti a necessità pratiche e amministrative con la volontà di transitare interamente documenti e processi al digitale – circostanza peraltro ancora *in fieri*, considerati da un lato lo stato di avanzamento della digitalizzazione delle pubbliche amministrazione e la rilevanza quantitativa delle modalità ibride –, dall'altro una visibilità limitata dell'archivio sia come *continuum* di fasi, sia delle necessità specifiche di ciascun passaggio, in particolare quelli di deposito e di conservazione permanente.

A proposito, in particolare nel testo delle Linee Guida, sarebbe necessaria una maggiore definizione, 'in parallelo' rispetto all'analogico, per le fasi di evoluzione dell'archivio: se

[1] Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 *Norme relative all'ordinamento ed al personale degli archivi di Stato.*

[2] Decreto Legislativo 22 gennaio 2004 n. 42 *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.*

possiamo, con le dovute cautele del caso, identificare l'archivio corrente nel sistema di gestione, non c'è altrettanta chiarezza sulle fasi di deposito e storico[3].

Vi è infatti fluidità nella scelta di collocazione dei documenti che hanno esaurito la loro funzione nei procedimenti di cui sono parte nel sistema di gestione piuttosto che nel sistema di conservazione[4]. L'attuale prassi predilige il versamento di tali documenti in conservazione, al fine di 'sigillarne' quanto prima le caratteristiche di autenticità, di integrità e immodificabilità: di fatto, secondo quanto definito prima dal DPCM 3 dicembre 2013 e dalle Linee Guida in seguito, i sistemi di conservazione devono prevedere il processo di scarto, le cui modalità sono indicate nei manuali di conservazione. Dunque, apparentemente, la normativa assegna ai sistemi di conservazione sia il ruolo di archivio di deposito sia di archivio storico[5].

L'appunto è sull'adeguatezza di tali identificazioni: sembra più appropriato conferire le funzioni di preservare la memoria a lungo termine a sistemi gestiti centralmente dalle istituzioni archivistiche, sul modello di quanto avviene nel caso dei Poli di conservazione e di quanto si vuole realizzare con il progetto dell'Archivio centrale dello Stato. Infatti, al di là dell'appartenenza e dell'afferenza dei documenti e degli archivi all'ambito pubblico o privato, è necessario stabilire processi e strutture in grado di accogliere, in delega o in custodia diretta, la documentazione destinata a costituire la memoria storica dei posteri: il *desiderata* è un progetto sviluppato nell'ambito del Ministero della Cultura che garantisca uno strumento comune – e allo stesso tempo scalabile sulle rispettive esigenze in merito al grado di riservatezza o di necessità di pubblicità della documentazione – per gli organi centrali del governo, gli altri ministeri e gli enti pubblici territoriali e non[6]. Questo anche in considerazione del fatto che nelle Linee Guida si indica che il Responsabile della

[3] Si rileva tale incertezza a partire dalle disposizioni del CAD: emerge, osservando le diverse modifiche del provvedimento, dai passaggi di accorpamento e separazione dei requisiti in materia di sistemi di gestione e di conservazione (si veda, in proposito, il capitolo II.2).

[4] Par. 4.1 *Linee Guida AgID* «Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD41,: a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito; b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica».

[5] F. Delneri, *Gli orizzonti della conservazione. Le tre età dell'archivio e il ruolo dei sistemi e degli istituti di conservazione*, , «JLIS.it Italian Journal of Library, Archives and Information Science», 10 (2019), 1, pp. 11-25, disponibile online al sito <https://www.jlis.it/article/view/12433/11357>.

[6] Per una trattazione più approfondita del tema si veda il paragrafo IV.2.3.

conservazione presso le amministrazioni statali centrali e periferiche ha l'obbligo di versare i documenti informatici, le aggregazioni informatiche e gli archivi informatici all'Archivio centrale dello Stato e agli Archivi di Stato territorialmente competenti, secondo quanto stabilito nel Codice dei beni culturali[7].

A tal proposito, si solleva una breve riflessione sulla scelta, ormai risalente a circa un decennio fa, di estendere la possibilità di affidare a soggetti terzi archivi e documenti pubblici, includendo in queste dinamiche il settore privato e, con esso, le implicazioni commerciali. Sebbene l'eventualità sia legata al rispetto di criteri e requisiti ben precisi, che forniscono garanzia di qualità e sicurezza dei servizi, sposta il focus delle considerazioni anche alla resa economica del prodotto e alle esigenze dei clienti. All'interno dei conservatori sono presenti figure con preparazione archivistica che effettuano valutazioni critiche e operative con cognizione di causa, ma vi è anche la necessità di rendere gli adeguamenti imposti dalla normativa meno impattanti per la propria comunità di utenti: si anticipa, a tal proposito, il tema dell'aggiornamento dei metadati minimi obbligatori che l'allegato 5 impone e dei formati dell'allegato 2, che implica modifiche di sistema per venire incontro alle esigenze di conformità delle PA, ma che devono essere estese e applicate anche a enti e aziende private, pur non sottoposti agli obblighi. Vi sono ulteriori conseguenze, tra cui si menzionano le variazioni contrattuali, le comunicazioni ai clienti e la diversificazione in soluzioni customizzate.

Sono interessanti, per la trattazione del tema, alcune precisazioni inserite nel nuovo Regolamento sulla qualificazione dei conservazione: lo scopo del provvedimento è stabilire i requisiti generali, di qualità, di sicurezza e organizzativi che devono possedere i soggetti, pubblici e privati, ai fini dello svolgimento del servizio di conservazione dei documenti informatici per conto delle pubbliche amministrazioni, ma restano espressamente esclusi servizi di conservazione a lungo termine disciplinati dal Codice dei Beni Culturali e le conseguenti attività di vigilanza e sanzionamento[8]. Tale affermazione implica la messa a disposizione di depositi cui si è già accennato, presumibilmente sviluppati nell'ambito dell'Ministero della Cultura: si ravvisa, dunque, il limite evidente di tale affermazione

[7] Par. 4.5 *Linee Guida AgID.*

[8] Art. 1 comma 1 *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici.*

nell'assenza di questi sistemi, dato che, appunto, lo spiraglio aperto con questa disposizione, è rappresentato ad oggi da un interrogativo. Si potrebbe pensare a un'ulteriore estensione del ruolo dei Poli, che peraltro assolvono già in parte a questa funzione.

Altri elementi lungimiranti da notare in relazione al contenuto del suddetto Regolamento sono la menzione della conformità alle raccomandazioni ETSI 319 401 e allo standard ISO 16363.

Il primo rappresenta un tentativo di allineamento con la normativa che disciplina la qualifica dei *Trust Service Providers* eIDAS e ben si inserisce nella scia delle novità della proposta di modifica di quest'ultimo: valutare un fornitore di servizi di conservazione con questo schema li colloca in prassi, se non ancora in diritto, tra gli erogatori di servizi qualificati fiduciari.

Altro passo verso l'apertura alle tendenze europee è l'inserimento dello standard ISO 16363: sebbene con l'incertezza delle modalità di presentazione dell'evidenza di conformità, rappresenta l'adesione a uno schema internazionale che consente di 'misurare' l'affidabilità di un deposito digitale, che incrementi la trasparenza in particolare sugli aspetti relativi agli accessi e agli accordi coi depositari[9].

Si menziona anche la novità dell'integrazione con il Servizio Pubblico di Identità Digitale, Carta di Identità Elettronica o altre identità digitali europee notificate: pur costituendo un punto interessante – peraltro già attuato presso il polo Marche DigiP, il quale prevede un meccanismo di autenticazione attraverso il Portale Servizi della Regione accessibile con SPID – si ravvede la necessità di chiarimento delle dinamiche e delle motivazioni di tale integrazione (si può ipotizzare un tentativo di evoluzione delle modalità di accesso), unita alla risoluzione delle sopracitate criticità, piuttosto che la proposizione di novità che determinino ulteriori implementazioni, anche onerose dal punto di vista delle risorse.

Il Regolamento, però, mostra i limiti e le situazioni indefinite di una soluzione di compromesso: nel (comprensibile) tentativo di tutelare i conservatori già accreditati, di

[9] M. Guercio, *La certificazione e i depositi digitali: il ruolo degli standard e delle linee guida*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 245-255, disponibile online al sito <https://journal.almamater.si/index.php/Atlanti/article/view/132/119>.

fornire riscontro alle osservazioni della Commissione europea e di anticipare l'associazione dei fornitori di servizi di conservazione ai *Trust service providers* eIDAS, si disciplina poco il transitorio e si profilano situazioni incerte.

In primo luogo, ci si riferisce all'ambito della Pubblica amministrazione: non è previsto l'obbligo, per soggetti terzi incaricati della custodia di documenti da essa prodotti, di iscriversi al Cloud Marketplace, ma è prescritto il rispetto dei requisiti elencati nell'allegato A, che sono quelli necessari per l'iscrizione alla sezione che sarà appositamente istituita all'interno del Marketplace per i conservatori. È evidente che si tratti di una situazione ambigua, cui si tenta un parziale rimedio con l'articolo 7, che afferma:

> 1) le amministrazioni che affidano il servizio di conservazione dei documenti informatici a soggetti non iscritti nella sezione "servizi di conservazione" del Cloud Marketplace 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 al presente regolamento.
>
> 2) L'Agenzia, fatte salve le sanzioni comminabili ai sensi dell'art. 32-bis del CAD, comunica senza indugio l'esito delle verifiche di cui al comma precedente all'amministrazione interessata che adotterà i provvedimenti conseguenti.

Fermo restando che si ipotizzi che la richiesta del contratto sia mirata a conoscere i dati identificativi del conservatore e gli accordi che intercorrono tra le parti (tempistiche comprese) – in luogo della documentazione altra relativa a organizzazione, strutture, misure di sicurezza fisica e logica e altri dettagli, poiché questi verranno richiesti in fase di verifica –, appare ci sia un certa possibilità sia evidente che un conservatore non risulti ancora iscritto al Marketplace poiché non ha ancora implementato o acquisito (o non ne ha l'intenzione) i requisiti dell'allegato A. Si sottolinea, infatti, che alcuni requisiti (per esemplificare, l'accesso al sistema con SPID), dal punto di vista tecnico risultano piuttosto onerose.

Per quanto riguarda il già citato inserimento di nuove raccomandazioni e standard, si nota che è genericamente menzionata una 'conformità', senza indicare checklist o matrici di riferimento su cui verrà verificata la *compliance* o le evidenze da produrre per effettivamente attestarla, lasciando di fatto (in questo caso, volutamente) indeterminato anche questo aspetto.

I punti di attenzione indicati riguardo al Regolamento 'ereditano' le criticità che si sono dovute affrontare con il passaggio in Commissione europea delle Linee Guida AgID: si comprende bene come dover trovare un compromesso tra la precedente situazione ormai rodata e ben definita dell'accreditamento e l'imposizione di rimuovere questo procedimento sia tutt'altro che semplice, a maggior ragione se si prevede di compiere questa operazione in tempi brevi. È proprio per tale ragione che si è tentato di tutelare i conservatori accreditati, inserendo requisiti che già possiedono, tra cui la conformità dei sistemi agli standard ISO/IEC 27001 ISO 14721 ed ETSI TS 101 533-1 v. 1.2.1, UNI SiNCRO per i pacchetti.

Al di là delle obiezioni sulla vicenda di pubblicazione del provvedimento, si ha comunque il vantaggio di uno strumento unitario sulla formazione, gestione e conservazione dei documenti informatici e che definisce in maniera chiara come questi debbano, in ogni fase, essere considerati nell'insieme delle relative aggregazioni e degli archivi in cui vengono prodotti, nell'ottica di preservare a lungo termine non singole entità, ma contesti[10]. Tra le altre note positive, vi sono maggiore definizione dei ruoli e delle responsabilità, in particolare in riferimento al ruolo di Responsabile della conservazione e Titolare dell'oggetto di conservazione: necessario però rilevare delle osservazioni dal Garante della privacy riguardo alla necessità di esplicitare maggiormente che è in capo al titolare (o al responsabile esterno, nel caso di conservatori) del trattamento l'obbligo di mettere in atto le adeguate misure di sicurezza fisica e logica[11]; il Garante, inoltre, evidenzia che sia insufficiente il richiamo generico ai principi di sicurezza in materia ITC nel testo delle linee guida e che è necessario definire dei regimi di autenticazione differenziati sulla base della tipologia di dati che si ha la facoltà di consultare. Anche riguardo al piano di sicurezza il Garante oppone troppa genericità nella definizione del contenuto, sostenendo che sarebbe necessaria una diversificazione dei livelli di sicurezza a seconda dei dati interessati dalla protezione.

Si evidenziano, infine, i già accennati problemi legati ai nuovi set di metadati e formati.

[10] Sul commento alle novità introdotte si veda L. Foglia, A. Lisi, *Conservazione dei documenti, ecco tutte le regole nelle linee guida AgID*, «Agenda Digitale», 15 settembre 2020, disponibile online al sito <https://www.agendadigitale.eu/documenti/conservazione-dei-documenti-ecco-tutte-le-regole-nelle-linee-guida-agid/>;

[11] Per le osservazioni sulla sicurezza dei sistemi di conservazione nelle Linee Guida si veda F. Ciclosi, *Le nuove linee guida AgID e il sistema di conservazione*, «ICT Security magazine», 17 aprile 2020, disponibile online al sito <https://www.ictsecuritymagazine.com/articoli/le-nuove-linee-guida-agid-e-il-sistema-di-conservazione/#_ftn28>.

Il primo, per quanto risulti completo rispetto alle necessità di gestione della Pubblica amministrazione, risulta sproporzionato per la conservazione e per l'ambito privato: sarebbe utile differenziare innanzitutto i metadati necessari alla gestione (per cui si sarebbe potuto optare per l'indicazione di seguire il modello suggerito dallo standard ISO 23081, in ottica di semplificazione) da quelli per la conservazione, per cui risulta sufficiente un corredo più ridotto ma più mirato, ad esempio desumibile dallo standard PREMIS[12]

Il secondo è estremamente dettagliato ed esaustivo, ma, per il fine cui è destinato, sarebbe risultato più efficiente un elenco meno caratterizzato ma comprendente i formati fondamentali (come nella normativa precedentemente vigente), con un rimando dinamico allo strumento PRONOM per informazioni aggiuntive e valutazione di casi particolari. Inoltre, si evidenzia l'utilità della presenza del formato .txt, ora assente, tra i formati consigliati: la sua semplicità e manipolabilità costituivano vantaggi importanti per la fase di conservazione.

Ultima, ma non per importanza, la problematica relativa alla poca definizione della fase di accesso e fruibilità dei documenti: si è scelta una conservazione 'chiusa', pensata per preservare l'integrità in senso stretto ma non a sviluppare la componente che permetta a comunità di utenti che vadano oltre al soggetto produttore e alle autorità che possano eventualmente chiedere la visualizzazione dei documenti di sfruttare le funzionalità di ricerca dei sistemi[13].

Vi sono ulteriori criticità se si pensa al contesto applicativo: non sono nominate sanzioni a danno dei soggetti che, negli effetti, non mettono in pratica le disposizioni, né vengono menzionati specifici controlli per verificare l'attuazione delle norme. Questi sono, oltretutto, assenti anche sulla qualità degli strumenti utilizzati e sulla reale presenza di figure professionali competenti e che ricoprano i ruoli stabiliti. Ciò, in ogni caso, si correla col fatto

[12] R. Vota, *L'opinione dei conservatori*, «Office automation. Tecnologie e modelli per il business digitale», 2 (2021), pp. 36-38, disponibile online al sito <https://www.soiel.it/sfogliabili/officeautomation/2021/febbraio-marzo/4QXjZdhY7q70qMyC.html#page=38>.

[13] Si riportano gli spunti di riflessione presentati nel corso dell'intervento di Maria Guercio in occasione del seminario 'Poli archivistici di conservazione digitale', tenutosi il 3 maggio 2021 nell'ambito dei 'Lunedì del Master', ciclo di seminari organizzati nell'ambito del master di II livello 'Formazione, Gestione e Conservazione di Archivi Digitali in ambito pubblico e privato' (i materiali sono disponibili all'interno della pagina dedicata del sito del Master al link <https://www.masterarchividigitali.unimc.it/poli-archivistici-di-conservazione-digitale-03-05-2021-seminario-online-a-cura-di-mariella-guercio/>).

che non si è nella pratica proceduto a guidare nella formazione e a sostenere finanziariamente le diverse realtà componenti la Pubblica amministrazione in questi processi. La possibilità di ricorrere a soggetti terzi, inoltre, giustifica le Pubbliche amministrazioni nell'avvalersi di vincoli contrattuali che facciano ricadere le responsabilità in capo ai fornitori di servizi.

In aggiunta, si ha poco la visione d'insieme del processo di conservazione, a partire dalle riflessioni che dovrebbero essere fatte già a partire dal momento della creazione dei documenti, che implica una mancanza di concezione di *policies* che siano funzionali a espletare correttamente le esigenze di tenuta a lungo termine delle risorse.

Si nota che

> il modello attuale non è in grado di gestire la natura complessa e dinamica della produzione documentale, della diversificazione dei tempi e dei modi d'uso dei documenti oltre che dei processi lenti della digitalizzazione che hanno portato a mostruosi e ingovernabili archivi ibridi, una delle difficoltà più importanti della conservazione di archivi (e non solo di documenti singoli sia pure metadati è la frammentazione presente nel soggetto produttore dovuta alla miriade di verticali che non sono intercettati dal sistema di gestione documentale e ancor meno dal sistema di conservazione: solo un servizio intermedio di archivio di deposito sarebbe in grado d L'inadeguatezza delle piattaforme di conservazione esistenti è evidente rispetto alla loro incapacità congenita di fornire una interfaccia aperta ai versamenti e, soprattutto, di acquisire la necessaria documentazione per la fruizione dell'archivio e non solo per l'esibizione a fini probatori di documenti informatici[14].

Per concludere, si riprende il severo (ma giusto?) parere espresso da Manlio Cammarata e riportato da Gilberto Marzano[15], secondo cui a una normativa complessa e dettagliata corrisponde un'abbondanza di interpretazioni e un'incertezza applicativa, su cui si innestano ulteriori dubbi sulle situazioni non disciplinate: del 2011 ma molto attuale, se si pensa ai già citati punti di discussione sulle Linee Guida.

Appare inadeguata, in quest'ottica, anche la forma frammentaria e secondaria delle disposizioni in materia di conservazione, ancor più se relazionata, come si vedrà nell'analisi comparativa, con le scelte di altre realtà: in un primo momento, le disposizioni in materia di conservazione discendevano dal CAD al DPCM 3 dicembre 2013, con specifiche sull'accreditamento delegate alla Circolare AgID 65/2014 e relativi allegati; attualmente, dal

[14] *Ibidem*.
[15] G. Marzano, *Conservare il digitale*, Editrice Bibliografica, 2011, pp. 225-229.

CAD si incanalano nelle Linee Guida AgID, con indicazioni sulla qualificazione contenute nell'apposito Regolamento, il quale, presumibilmente, verrò corredato con ulteriori *checklist*. Appare, in tale contesto, difficile orientarsi tra le disposizioni, parte delle quali, come si è visto, contengono anche delle situazioni indeterminate.

Il rapporto del contesto italiano con le esperienze europee

Lo scopo a cui evidentemente si tende in ambito europeo è la condivisione e la semplificazione: il punto di forza delle esperienze internazionali è la volontà di disporre di linee guida e strumenti comuni, realizzata con la messa a disposizione pubblica di specifiche, documenti e soluzioni e la discussione a riguardo in occasioni divulgative, anche in fase sperimentale, in modo tale da trarre vantaggio dai riscontri della comunità di riferimento, composta tanto da professionisti quanto da utenti finali che non possiedono competenze specifiche in materia.

Parte di queste iniziative sono sostenute da progetti e finanziamenti della Comunità europea, a testimonianza dell'importanza che il tema della conservazione digitale riveste ormai da oltre un quindicennio. Da parte di quest'ultima, nonostante non ci siano regolamenti né direttive che disciplinano l'argomento, si ha comunque l'evidenza di ricondurre ad un minimo comune denominatore le prassi: non ultima, in proposito, l'inclusione dei servizi di conservazione tra i *trust services* nella proposta di modifica al Regolamento eIDAS.

In Italia manca, per certi versi, quest'ottica di inclusività: sebbene sia evidente la volontà all'apertura e all'allineamento di disposizioni al contesto europeo, ad esempio con l'inserimento nelle nuove Linee Guida dello standard ETSI 319 401 o con le modifiche a UNI SiNCRO relative all'utilizzo dell'inglese per un'auspicata adozione internazionale, c'è una tendenza nella pratica a ragionare entro i propri confini. Evidenze di questa affermazione sono i già citati casi dei nuovi allegati sui metadati e sui formati delle linee guida; si è già accennato come nel primo caso si sarebbe potuto distinguere tra metadati di gestione e di conservazione, riducendo il set per questo ultimo scopo e adeguandoli entrambi a standard

internazionali; nel secondo caso si sarebbe potuto procedere a semplificare gli schemi utilizzando il modello PRONOM[16].

Quello che, inoltre, sarebbe necessario si apprendesse dalle esperienze europee è l'interesse per la sensibilizzazione al tema di tutti i tipi di produttori di patrimonio documentale, da cui passa la presa di coscienza dell'importanza della gestione e conservazione di tali beni, che innesca la conseguente pianificazione di strategie adeguate e implementazione di sistemi performanti: al di là della norma e dell'obbligo, le associazioni, le iniziative e i progetti, oltre agli aspetti legati alla ricerca, si occupano anche di veicolare informazioni che vadano dalla veduta ad alto livello sull'argomento all'approfondimento in base al contesto, e di fornire strumenti utili come guide all'elaborazione di strategie o software veri e propri. Di qui, la grande importanza attribuita nelle discussioni in ambito europeo alla fase di *planning*, in relaziona a cui si è visto come associazioni e gruppi di lavoro[17] si adoperino per creare strumenti che consentano di impostare correttamente obiettivi e flussi di lavoro.

Nel contesto italiano, l'interesse è mosso, in sostanza, dal carattere mandatorio delle disposizioni: in particolare in ambito privato, ci si occupa di conservare i propri documenti digitali nella misura in cui, per vincoli legati a necessità giuridiche o fiscali, sono oggetto di tempi e modalità di conservazione prestabiliti. Nel caso dell'ambito pubblico, il problema si collega all'inversione 'cronologica' tra sensibilizzazione al problema e imposizione del vincolo: si pongono le regole prima di aver effettuato, in via preventiva e proattiva, interventi che agevolino la conoscenza del tema e facilitino il passaggio dalla conservazione di archivi analogici a quelli digitali. In sostanza, la preparazione degli 'addetti ai lavori' non è condizione sufficiente per un'adeguata gestione delle attività inerenti alla conservazione digitale: data la necessità di concepire la tenuta a lungo termine dalla formazione dei

[16] Si menziona in nota che altra dimostrazione chiara di è il fatto che le uniche presenze italiane che si registrano per la partecipazione alla conferenza iPRES sono relative all'ambito accademico (peraltro, non troppo numerose) e assenti sono associazioni, enti e organizzazioni; in rappresentanza di altre nazioni (benché, in alcuni casi, anche più ridotte dell'Italia per dimensioni e popolazione), risultano figure provenienti da istituzioni archivistiche e aziende private, tra cui figurano anche i responsabili della realizzazione dei progetti che si menzionano nei casi di studio.

[17] Si citano, a scopo esemplificativo, la guida *Engaging decision makers* della DPC e i *Levels of Preservation* della NDSA (si veda il capitolo I.3).

documenti e degli archivi, è fondamentale che chi si occupa della loro produzione sia adeguatamente preparato a svolgere il proprio compito e a intenderne lo scopo.

L'esempio dei Poli di conservazione

Esperienza positiva di convergenza tra riflessioni e pratica sono i Poli di Conservazione.

Innanzitutto, nel già menzionato documento *Progetto Poli di conservazione*[18] emergono spunti interessanti, tra cui la definizione, in maniera riassuntiva e chiara, dei tre cardini su cui dovrebbero incentrarsi normativa e applicazioni effettive; la conservazione, infatti, deve:

> 1. essere incentrata non sui singoli documenti digitali ma sulle loro aggregazioni e sulle relazioni stabili che le definiscono (per esempio fascicoli e serie digitali) nella fase di formazione e gestione documentale, anche se nel caso di un trasferimento immediato non tutte le informazioni necessarie sono disponibili [..];
>
> 2. disporre di documentazione sufficiente a ricostruire (in modo auto-consistente) l'originario sistema di produzione (incluse le informazioni sugli organigrammi, sui criteri e metodi di profilazione degli utenti, le indicazioni organizzative e operative presenti nei manuali di gestione), fornendo indicazioni sui criteri di ordinamento degli archivi e sulle regole di organizzazione interne agli enti;
>
> 3. essere esercitata, nel caso degli archivi pubblici, da istituzioni che, compatibilmente con i principi del nostro ordinamento giuridico e con il modello attuale di tutela archivistica, possano assumere in forme adeguate la responsabilità di interventi di custodia attiva, che in alcuni casi non potrà non implicare modifiche ai bit originari trasformando di fatto e inevitabilmente la conservazione di documenti originali in conservazione di copie autentiche dei documenti e delle loro componenti, la cui conformità all'originale dovrà essere debitamente attestata[19].

Riguardo a questo ultimo punto, in particolare, viene operata nel documento una distinzione tra la conservazione a termine e permanente è supportata dalle evidenze della prassi e dello 'storico', individuando il discrimine tra le due tipologie di conservazione nella comunità di riferimento e nelle relative modalità di accesso ai documenti e nell'esigenza di mantenimento dell'autenticità da un *range* prescritto dalla legge a una prospettiva illimitata; nel primo caso è sufficiente determinare le dinamiche di consultazione ed estrazione di copie

[18] Si veda il capitolo II.3.

[19] *Progetto Poli di conservazione. Definizione di un modello di riferimento per i Poli di Conservazione e della relativa rete nazionale*, disponibile online al sito <https://www.agid.gov.it/sites/default/files/repository_files/definizione_di_un_modello_di_riferimento_per_i_poli_di_conservazione_e_della_relativa_rete_nazionale_0.pdf>, p. 17.

col soggetto produttore, prevedendo inoltre meccanismi di monitoraggio sui documenti che permettano di verificare la consistenza delle sue proprietà per un periodo limitato; nel secondo caso vanno presi in considerazione i cambiamenti tecnologici che possano intervenire in un futuro significativamente distante, con la necessità che vengano trasmesse tutte le informazioni volte a testimoniare eventuali passaggi di custodia e trasformazioni, per garantire la longevità delle caratteristiche del documento e la sua leggibilità. È proprio per tale ragione che la conservazione a lungo termine delle memorie digitali, come di quelle analogiche, viene ritenuta prerogativa di istituzioni pubbliche, incaricate di salvaguardare il patrimonio per i posteri, poiché:

> La conservazione permanente non può ignorare che quanto più si allunga la dimensione temporale tanto più la comunità degli utenti muta sia nella sua composizione prevalente sia per quanto riguarda la base di conoscenze implicite possedute[20].

La soluzione si vede proprio nei Poli di Conservazione: ognuno di questi

> si configura come uno o più soggetti che, ai fini della conservazione secondo le norme vigenti, condividono o forniscono risorse organizzative, procedurali, strumentali, tecnologiche, economiche ed umane in collaborazione o a favore di enti e amministrazioni pubbliche responsabili della produzione di quei documenti e archivi e giuridicamente titolari della loro conservazione e interessati al loro utilizzo futuro[21].

Rispondono, dunque, a tutte le esigenze sopra menzionate, a maggior ragione se li si raccoglie in una struttura di Rete, che, in quanto tale, consente interoperabilità, collaborazione e supporto sia reciproco sia verso le autorità di vigilanza.

Questo documento è espressione di riflessioni dal punto di vista archivistico, generate dal vaglio di esperienze pratiche e adeguate al contesto, che sembrano, però, non trovare riscontro nell'elaborazioni della normativa e di una strategia comune per la conservazione a lungo termine delle memorie pubbliche provenienti da tutte le tipologie di enti e da tutto il territorio.

Comunque, per esemplificare le realizzazioni concrete con gli scenari considerati, si evidenzia come il Polo ParER, ad oggi, raccolga la gran parte dei documenti delle

[20] Ivi, p. 19.
[21] Ivi, p. 20.

amministrazioni dell'Emilia Romagna e costituisca un unico punto di accesso per tutta la documentazione, compresa quella più complessa come i piani urbanistici o le evidenze sanitarie. Inoltre, si sta riflettendo sulle modalità di integrazione con il Portale SAN (Servizio Archivistico Nazionale[22]), per rendere il patrimonio conservato consultabile e fruibile da parte dell'intera comunità di utenti.

Il Polo Marche DigiP vanta un grande investimento sulla considerazione della comunità di riferimento e sui processi di verifica della qualità di ciò che viene versato, puntando su una particolare personalizzazione degli accordi sulla base dell'ente specifico di riferimento e sull'implementazione di sviluppi e modifiche sulla base del riscontro che questi ultimi forniscono in apposite occasioni di confronto. Si evidenzia anche un'apertura all'utilizzo di strumenti internazionali, in quanto il controllo dei documenti viene effettuato attraverso FITS.

Un ostacolo da superare, però, è costituito dal fatto che questi Poli non abbiano una funzione istituzionale: si presentano come conservatori accreditati, non come custodi di memoria pubblica con apposito mandato come l'Archivio Centrale dello Stato. Quest'ultimo, in proposito, costituirà un primo esempio di Polo con questa prerogativa: il progetto *Polo di conservazione dell'ACS* (PCACS) costituirà un *repository* degli archivi degli organi centrali dello Stato, che presenterà il vantaggio di essere frutto di esperienza ragionata non solo dei Poli di conservazione, ma anche delle iniziative internazionali.

Si ritiene, in conclusione, che i Poli siano la chiave per la realizzazione di 'conservatori pubblici' che siano realmente tali, che costituiscano l'equivalente di quello che sono gli Archivi di Stato per i documenti analogici e che, anzi, che ne rappresentino un ulteriore sviluppo, come parte funzionale di queste ultime strutture, integrata in ottica di continuità rispetto alla gestione. Si vedrà, inoltre, come queste esperienze ben si collocano tra i modelli implementati negli altri casi di studio rappresentati nell'elaborato[23].

La conservazione digitale e le *Digital humanities*

[22] <http://san.beniculturali.it/web/san/home>.
[23] Si veda, a riguardo, il paragrafo IV.2.3.

In questa sede, in conclusione, merita un accenno l'inserimento del tema conservazione digitale all'interno del contesto delle *Digital humanities.* Il quesito di base è: che rilevanza riveste la conservazione digitale all'interno di questo dominio? A prescindere dal dibattito, attualmente molto sentito e intenso, sull'effettivo raggio d'azione coperto dal cappello delle *discipline umanistiche digitali* e sul livello su cui si dovrebbe assestare la competenza delle figure tradizionalmente *umanistiche* dal punto di vista informatico e tecnologico, risulta che poco spazio sia dedicato alla trattazione degli archivi digitali: questi, meno 'esplorati' rispetto a temi legati alla linguistica computazionale, al *text mining* e alla codifica del testo, sono rappresentati, principalmente, da progetti di digitalizzazione di contenuti analogici e relativa descrizione – per la messa a disposizione del patrimonio risultante – dei set di metadati utilizzati ai fini della ricercabilità e dell'accessibilità delle risorse e dell'interoperabilità di queste ultime per l'utilizzo in diversi sistemi informativi[24].

Per identificare una casistica, si fa riferimento ai principi FAIR[25]: questi *Guiding principles* – il cui acronimo sta per *findable, accessible, interoperable, reusable* – forniscono indicazioni sulle modalità di predisposizione di dati, metadati e infrastrutture, perché siano, accessibili, interoperabili, ricercabili e riusabili. Sono ampiamente utilizzati dalla comunità delle *Digital humanities* e discusse in ogni sfaccettatura teorica e pratica, ma presentano il limite evidente di non porre nessuna attenzione alla conservazione a lungo termine degli oggetti trattati.

Premettendo che quasi del tutto assenti restano anche tanto la parte di cura corrente della documentazione nativa digitale e quella dedicata alla fase che precede la conservazione permanente, si nota che la discussione sulla conservazione a lungo termine avviene in contesti diversi, su tavoli legati alla digitalizzazione della Pubblica amministrazione o in ambiti strettamente settoriali[26]. Vi è, però, da dire che gli aspetti relativi alla conservazione

[24] Per dare evidenza di tali affermazioni è sufficiente consultare i programmi delle ultime edizioni di alcuni tra i più noti convegni sul tema, ovvero il Convegno annuale AIUCD (per il 2020 al link https://aiucd2020.unicatt.it/aiucd-programma>, per il 2021 al link <https://aiucd2021.labcd.unipi.it/programma/>) e della Conferenza annuale DH Benelux (per il 2019 al link <https://web.archive.org/web/20210303082329/https://2019.dhbenelux.org/program/>, per il 2021 al link <https://2021.dhbenelux.org/schedule/>)

[25] I.J. Aalbersberg, G. Appleton, M. Dumontier et al, *The FAIR Guiding Principles for Scientific Data Management and Stewardship*, «Scientific Data», 3 (2016), pp.1-9, disponibile online al sito <https://doi.org/10.1038/sdata.2016.18>.

[26] Si rimanda, in proposito, al capitolo II.1.

digitale discussi nelle sessioni a tema *Digital humanities* rivestono interesse in quanto possono essere considerati complementari rispetto alle carenze in normativa: che si tratti di risorse digitalizzate o generate elettronicamente, si approfondisce in particolare come poter rendere fruibile tale patrimonio a una vasta comunità di utenti, a supporto non solo di ricerche e studi accademici, ma di qualsivoglia scopo[27].

[27] Ci si riferisca, a titolo esemplificativo, agli interventi P. Ciuccarelli, M. Mauri, *Il ruolo dell'*Information Visualization *nella progettazione di interfacce per archivi digitali eterogenei*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare,* Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 73-88; P. Feliciati*, Convergere a valle. Lo studio del punto di vista degli utenti degli ambienti culturali digitali e l'esperienza del progetto "Una Città per gli Archivi"*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare*, Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 89-112; F. Mambelli, *Una risorsa online per la storia dell'arte: il database della Fondazione Federico Zeri*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare*, Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 113-125.

IV.2 Il panorama italiano in rapporto agli stati europei analizzati

Il contesto dei singoli Stati europei – emerge dalle descrizioni dei casi di studio – è molto diversificato dal punto di vista istituzionale e amministrativo, delle competenze sulle questioni archivistiche, delle disposizioni normative in materia e delle soluzioni organizzative, tecniche e operative adottate.

Si è già notato come l'Italia parta da una base normativa e archivistica molto sviluppata e da buone pratiche già in uso, che i Paesi europei presi in esame non possiedono o hanno implementato in maniera più puntuale[1]: le differenze sono molteplici e vanno valorizzate, al fine di tracciare prospettive, ipotizzare modelli condivisibili su larga scala o, viceversa, comprendere le ragioni per cui eventuali schemi non si possano applicare a realtà differenti.

Vi sono, preliminarmente, delle osservazioni necessarie collegate al contesto generale di riferimento degli Stati selezionati come casi di studio[2]. L'Austria e l'Olanda rappresentano realtà in cui è possibile una gestione degli affari amministrativi è fortemente centralizzata, per la forma di governo, per l'estensione territoriale e la sua organizzazione e per il numero di abitanti[3]: questo implica una produzione di documenti e di evidenze minore e la gestione di flussi diversi rispetto alle dinamiche italiane e francesi.

La Francia, sulla base degli stessi criteri quantitativi e qualitativi generali citati per l'esempio austriaco e quello olandese, presenta un quadro più affine a quello italiano: la gestione dei procedimenti amministrativi avviene per lo più in maniera decentralizzata, attraverso una rete corposa di enti e uffici che producono documenti afferenti al proprio

[1] Sulle considerazioni generali relative al confronto tra il contesto italiano e altri Paesi comunitari si vedano anche M. Guercio, *Conservare il digitale: modello nazionale e contest*

o internazionale, «DigitCult – Scientific Journal on Digital Cultures», 1 (2016), 2, pp. 19-26, disponibile online al sito <https://digitcult.lim.di.unimi.it/index.php/dc/article/view/10/10>; G. Marzano, *Conservare il digitale*, Editrice Bibliografica, 2011, pp. 213-225.

[2] Si faccia riferimento, per relazionare questo tema con le forme di governo, al paragrafo III.1.

[3] In termini numerici, l'Austria ha una popolazione di 8 932 664 persone su una superficie di 83 879 km2, la Francia ha una popolazione di 67 439 599 individui su una superficie di 633 186,6 km2, l'Italia ha una popolazione di 59 257 566 individui su una superficie di 302 073 km2, l'Olanda ha una popolazione di 17 475 415 individui su una superficie di 41 540 km2, la Romania ha una popolazione di 19 186 201 individui su una superficie di 238 390,7 km2 (si vedano, in proposito, le pagine dedicate ai dati quantitativi delle nazioni parte dell'Unione europea sul proprio sito istituzionale al link <https://europa.eu/european-union/about-eu/figures/living_it#size> per i dati sulla superficie, al link <https://europa.eu/european-union/about-eu/figures/living_it#population> per la popolazione).

dominio territoriale o funzionale, per far fronte alle esigenze della seconda popolazione europea più numerosa.

La Romania, infine, mostra un contesto particolare rispetto ai precedenti: dalle dimensioni intermedie rispetto ai già citati esempi, presenta in relazione a questi una densità di popolazione più bassa, che la rende per certi versi affiancabile al contesto austriaco, ma una rete distrettuale simile a quella francese.

IV.2.1 Contesto istituzionale e amministrativo

Per quanto riguarda l'aspetto specifico della distribuzione delle competenze relative all'ambito della conservazione digitale nei casi descritti si nota, in primo luogo, una naturale divisione delle stesse tra autorità archivistiche ed enti che trattano la digitalizzazione delle strutture statali amministrative: ciò su cui si osservano variazioni è la preponderanza della prima sulla seconda e viceversa, con una direttamente proporzionale adeguatezza delle disposizioni vigenti in materia e della qualità dei progetti implementati.

La coordinazione è la chiave per l'elaborazione di strategie funzionali: in Francia il 'dominio' sulle questioni relative alla conservazione della memoria documentale, sia analogica sia digitale, è in capo al *Service Interministériel des Archives de France*: questo fornisce le direzioni e le indicazioni da seguire per il versamento e la conservazione dei documenti pubblici (svolgendo anche attività di controllo sugli archivi correnti) e si coordina con la *Direction interministérielle du numérique et du système d'information et de communication de l'État* per la realizzazione di progetti allo scopo di garantire una corretta tenuta degli archivi *intermédiaires* e *définitives*.

Altro analogo caso positivo è rappresentato dall'Olanda: ciò che concerne la conservazione delle risorse digitali è prerogativa del *Ministerie van Onderwijs, Cultuur en Wetenschappen*. Questo, attraverso l' Ispettorato per l'informazione e il patrimonio culturale si assicura che i documenti e gli archivi siano correttamente predisposti alla conservazione permanente, mentre attraverso i *Nationaal Archief* realizza le strutture necessarie al mantenimento a lungo termine delle risorse digitali, sviluppate da figure con una preparazione prettamente archivistica che si avvalgono dei riscontri della comunità di riferimento e delle esperienze internazionali.

La legge austriaca conferisce estese funzioni in materia archivistica all'l'*Österreichisches Staatsarchiv*, che funge da collettore degli archivi di deposito e storico del governo federale e si è occupato dell'implementazione del sistema di conservazione statale DigLA, mentre il *Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt* si occupa principalmente di guidare la digitalizzazione dei processi che avvengono in fase di produzione e gestione della documentazione, in particolare in riferimento alle relazioni col cittadino.

Si è già accennato, invece, come in Italia, le principali funzioni normative e di vigilanza sui conservatori sono attribuite all'Agenzia per l'Italia Digitale. Ciò che resta, sostanzialmente, compito del Ministero della Cultura, tramite l'azione della Direzione Generale degli Archivi, gli Archivi di Stato e le Soprintendenze archivistiche, è la tutela sugli archivi pubblici, che si esplicita, di fatto, semplicemente nella facoltà di ispezionare il patrimonio culturale documentale[4] e nell'obbligo, per i soggetti produttori pubblici o privati che possiedano un archivio dichiarato di interesse storico, di sottoporre all'autorizzazione del Ministero lo scarto dei documenti[5].

Questa tendenza di 'distanziamento' delle autorità archivistiche è portata alle estreme conseguenze nel caso della Romania: a scapito degli *Arhivele Naţionale ale României* – che peraltro ricade sotto la direzione del Ministero dell'Interno – l'ambito delle memorie digitali è collocato tra le competenze dell'*Autoritatea pentru Digitalizarea României* e, prima di quest'ultimo, del *Ministerul Comunicaţiilor şi Societăţii Informaţionale*. Questo ha implicato la redazione di provvedimenti e l'impostazione di prassi che non hanno fondamenta archivistiche e, dunque, si rivelano non particolarmente adeguate a raggiungere il finale scopo del tramandare ai posteri un patrimonio documentale accessibile e utilizzabile.

IV.2.2 Disposizioni normative

Gli approcci dei legislatori austriaco, francese, italiano, olandese e rumeno in relazione alla tracciatura di un perimetro normativo sulla conservazione digitale mostrano reazioni differenti e l'adozione di diverse soluzioni.

[4] Art. 12 DL. 42/2004.
[5] Art. 19 DL. 42/2004.

Si è visto come l'Italia abbia gestito la forma e il contenuto della normativa di settore: a tal proposito, si rileva l'adozione di soluzioni più funzionale da parte dell'Olanda e della Francia, sulla scorta di quanto già affermato nel precedente capitolo riguardo alla ridondanza e all'eccessivo dettaglio della normativa. La linea scelta da queste due nazioni è l'allineamento delle disposizioni primarie in materia di patrimonio culturale e archivi: in Francia il Codice dei beni culturali è stato revisionato in funzione dell'introduzione delle tecnologie in ambito archivistico, così come in Olanda è stata riformulata la Legge archivistica. Tali revisioni non vincolano in maniera stringente i requisiti in termini tecnologici e i processi interni ai sistemi, ma forniscono dei riferimenti cardine validi a disciplinare uniformemente e con dispositivi di legge principali la conservazione delle memorie digitali. Questo approccio si rivela non solo lungimirante, ma mostra una sensibilità sulla considerazione in continuità e in compresenza delle dimensioni analogica e digitale, fornendo anche, in particolare nel caso francese, confini più netti tra le diverse fasi di vita degli archivi – anche in parallelo rispetto agli stessi concetti in ambito cartaceo – e, conseguentemente, direzioni più precise in relazione ai passaggi di stato della documentazione.

La Romania, costituisce da un lato un esempio di precocità nell'adozione di norme specifiche in materia di archiviazione elettronica, ma, pur celere nel dotarsi di quest'ultime, rispecchia un'estremizzazione della dicotomia amministrativo culturale cui si è più volte accennato: le autorità archivistiche restano praticamente escluse da ciò che riguarda l'elaborazione delle disposizioni di legge e dalle prassi di accreditamento di soggetti terzi che intendono prestare servizi di archiviazione. Si è già notato come questo termine venga usato in maniera vaga rispetto alle fasi di gestione e conservazione: quando, infatti, gli Archivi Nazionali sono stati consultati per la Legge del 2007, il contributo apportato non è stato significativo, essendo ritenute le memorie digitali da alcuni archivisti non di propria competenza. La Legge sull'archiviazione elettronica, in Romania:

> looks a sort of mixture of specifications for ERMS, OAIS-compliant systems and Trusted Digital Repositories, without fully covering any of them. Reserving the right of inspection over electronic archive to the Ministry for Information Society was a relief for the National Archives, but, on long term, it is expectable to create a real trouble for the permanent records.

> On the other hand, the real life does not fit with the intentions of the regulator. In June 2015, according to the Registry for Electronic Archiving Operators (Internet 17), after 7 years from the enforcement of the law, there are only 14 operators, and only 3 for "their own archives". That would mean in Romania, legally speaking, there are only 14 creators of electronic archives, all the other institutions relying on paper records - which is absurd[6].

Riguardo alla disciplina sul ricorso all'esternalizzazione, la tendenza positiva, in particolare se ci si riferisce al patrimonio culturale da conservare perennemente, è minimizzare il ricorso a soggetti terzi operanti nell'ambito privato. L'Italia, su questo tema, rappresenta un caso intermedio tra le realtà considerate: l'Austria e l'Olanda, per le ragioni già espresse, sono nelle condizioni di poter optare per una strategia centralizzata che esclude il ricorso a terze parti; la Romania, in assenza di un sistema sviluppato in coordinazione tra autorità archivistiche e ADR, presenta nel proprio corredo normativo disposizioni finalizzate principalmente alla cessione del servizio a soggetti appositamente designati (pur essendo prevista la possibilità, per gli enti governativi, di sviluppare *in house* il proprio sistema).

La similitudine più evidente si trova col caso francese: sebbene con l'obiettivo di minimizzare l'intervento di soggetti esterni (per la verità più evidente nel caso francese[7]), si avverte la necessità di normare anche questa eventualità, al fine di garantire la qualità dei servizi di cui le Pubbliche amministrazioni possano usufruire. Lo schema di qualificazione francese presenta un meccanismo più snello rispetto a quello attualmente in vigore in Italia: subordina la qualificazione all'ottenimento (seppure economicamente oneroso) della certificazione NF 461 e consente l'esercizio a seguito dell'autorizzazione del prefetto di competenza territoriale. Sebbene tanto l'Italia quanto la Francia abbiano adeguato le proprie disposizioni alle esigenze espresse in contesto europeo (anche, ad esempio, sulla rimozione dell'obbligo di localizzazione dei dati in territorio nazionale), quest'ultima ha percorso una strada di snellimento dei processi di qualificazione dei conservatori, ponendo come unico fondamentale prerequisito per l'autorizzazione da parte del prefetto a prestare servizi per i soggetti pubblici la presenza della certificazione NF 461.

[6] B-F. Popovici, *Electronic Records Management in Romania, cit.,* pp. 189-190.

[7] Si vedano, in proposito, i riferimenti numerici relativi ai conservatori esterni accreditati o autorizzati al capitolo II.2 e al paragrafo III.3.3.

Un tentativo di semplificazione delle dinamiche è il processo introdotto dal *Regolamento sui criteri per la fornitura dei servizi di conservazione*: l'iscrizione dei servizi alla Piattaforma Cloud dedicata si avvicina, in alcuni punti, al paradigma austriaco sull'acquisizione del sigillo *Ö-Cloud*. Questo, estrema semplificazione, costituisce allo stesso tempo potenziale spunto per risolvere le obiezioni poste dalla Commissione europea sulla procedura di accreditamento, non potendo vincolare alcun obbligo per via del parere circostanziato: lo schema di autovalutazione per servizi cloud costituisce un elemento ben mirato sui requisiti, reso oltretutto pubblico, che consente trasparenza verso la comunità di utenti e rappresenta lo strumento revisionato dall'autorità competente per la concessione dell'apposito sigillo.

IV.2.3 Strumenti, modelli e standard

L'analisi delle soluzioni sviluppate per garantire la conservazione dei documenti digitali nell'ambito dei casi di studio considerati rivela degli approcci interessanti e positivi per diverse ragioni: in primo luogo, poiché vi è il tentativo di realizzare dei sistemi collettori sviluppati nell'ambito di progetti gestiti dalle autorità archivistiche in coordinamento con gli organi preposti alla digitalizzazione, a scapito della delega a soggetti terzi e al ricordo all'esternalizzazione; in secondo luogo poiché lo sviluppo di soluzioni concrete dà modo di poter realizzare negli effetti una conservazione digitale sostenibile e interoperabile: al di là dell'adozione ormai pressoché assoluta dell'architettura OAIS, l'utilizzo di strumenti e modelli condivisi ed elaborati nell'ambito della ricerca europea consente la creazione di pacchetti dalla struttura uniforme, che implica possibilità di automatismi per lo scambio delle informazioni e, disponendo di un'ampia comunità di utilizzatori, le garanzie di aggiornamento costante e di supporto nella risoluzione dei problemi.

Tali sono le proposte di Austria e Olanda che, con DigLA ed e-Depot: queste piattaforme, finalizzate esplicitamente alla conservazione del patrimonio documentale digitale, sono sviluppate entrambe nell'ambito degli Archivi Nazionali, che ne curano la gestione, il monitoraggio e le modifiche e fanno uso di componenti implementate nell'ambito delle organizzazioni internazionali.

È necessario, però, ribadire le caratteristiche dimensionali e organizzative di Austria e Olanda: per questi Stati è più ampia, rispetto all'Italia e alla Francia, la fattibilità di

realizzazione di modelli centralizzati per la raccolta dei documenti: si nota, innanzitutto, dalle modalità definite dalla legge per le procedure di selezione e scarto e di versamento, in cui le autorità archivistiche svolgono un ruolo centrale e di cooperazione con i soggetti produttori pubblici.

È da notare che i sistemi centralizzati olandese e austriaco hanno considerato l'accesso alle risorse come una delle priorità sin dal momento della progettazione: questi Paesi danno evidenza di come intendono garantire la facoltà alla comunità di utenti di poter usufruire del patrimonio documentale da essi conservato attraverso moduli di accesso di DigLA ed e-Depot appositamente predisposti alla consultazione pubblica.

In Francia, invece, si è optato per una soluzione (più consona anche a una potenziale applicazione italiana) che mira sempre all'utilizzo diffuso di uno strumento comune e 'centralizzato' per tutta la pubblica amministrazione, ma per cui viene lasciata più libertà di implementazione ai singoli organi ed enti di riferimento e la possibilità di integrarsi con i propri sistemi gestionali. Alla realizzazione di un unico sistema per tutte le amministrazioni, si è preferito lo sviluppo di un software scalabile, la cui diffusione è accompagnata da bandi di finanziamento che non solo includono supporto economico, ma anche in termini di formazione, allo scopo di dotare delle corrette competenze e aumentare la consapevolezza delle figure incaricate allo svolgimento delle attività di integrazione e conservazione rispetto al fine ultimo di conservazione del patrimonio culturale.

In Italia, la situazione è definita ad alto livello nei documenti programmatici come i Piani Triennali, ma 'frammentaria' dal punto di vista delle applicazioni concrete: si può identificare un parallelo agli esempi dei casi di studio nei Poli di conservazione, in particolare nel progetto di Polo ACS, con delle dovute precisazioni, dato che si ha comunque la mancanza di un piano coerente che coinvolga l'intera Pubblica amministrazione.

Questi, infatti, riflettono un esempio di tentativo di implementazione di struttura pubblica per la conservazione, ma, come già affermato, hanno il limite di non avere un mandato istituzionale di collettori di memorie riconosciuto a livello normativo e di dover essere, in ogni caso, sottoposti a procedure di accreditamento e qualificazione come i soggetti operanti nel settore privato. Per il momento, i Poli attivi riflettono ancora realtà territoriali o circoscritte a un ente di riferimento e hanno la caratteristica di potersi 'autodeterminare' nelle

scelte organizzative e tecnologiche, rispetto unicamente alla normativa di settore. È inoltre frequente, da parte dei piccoli enti, affidare il servizio di conservazione in esternalizzazione, sia per esigenze pratiche sia per la partecipazione a esito positivo dei fornitori a bandi di gara.

Il progetto per il Polo ACS, però, rappresenta una futura prospettiva positiva per cominciare a superare i limiti esposti e per la costituzione di un modello esportabile anche sulla rete di Archivi di Stato, mettendo in pratica una soluzione intermedia tra gli esempi DigLA, e-Depot e VITAM. Non solo, infatti, l'ACS possiede le specifiche funzioni istituzionali, ma sta portando avanti, in fase progettuale, un vaglio delle esperienze internazionali; sono stati valutati, come si è detto, l'esempio francese e eARK, a vantaggio di quest'ultimo: scegliere di aderire a tale modello significa andare incontro alle tendenze europee di uniformità e cercare di superare i limiti del quadro nazionale.

È importante, infine, evidenziare un elemento positivo comune delle soluzioni austriaca, francese, italiana e olandese: l'evoluzione e l'aggiornamento degli strumenti, oltre che dalle valutazioni tecniche, sono basate sui *feedback* della comunità di utilizzatori e di utenti finali, a garanzia della qualità dei sistemi e della loro effettiva rispondenza alle necessità delle categorie interessate.

Per concludere, tenuto conto delle dovute differenze contestuali, per una realtà come quella italiana la prospettiva ideale è una soluzione che preveda per la fase di deposito uno strumento come VITAM, che consenta agli enti pubblici e ai ministeri di occuparsi in prima battuta della conservazione dei propri documenti: in questo modo, disporrebbero dell'idoneo supporto finanziario e formativo nel percorso di digitalizzazione e conservazione e di uno strumento che consenta di occuparsi della tenuta delle proprie risorse sino ai momenti di selezione e scarto compresi in autonomia, ma che allo stesso tempo sia sotto il controllo dell'autorità archivistica per quanto riguarda la definizione dei pacchetti e dei metadati, la definizione delle *policies*, la manutenzione e l'aggiornamento del software.

Per gli archivi storici digitali, invece, è auspicabile lo sviluppo di una soluzione analoga a DigLA ed e-Depot (circostanza che, come già descritto, sta già in parte realizzandosi con il progetto del Polo ACS), che faccia riferimento alla rete di Archivi di Stato, per fare in modo che permanga comunque la gestione dei processi sul piano territoriale, ma che si

disponga di un unico *repository*, sfruttando le possibilità descritte dallo standard ISO 14721 sull'interoperabilità e la cooperazione applicativa tra archivi OAIS.

Conclusioni

Digital preservation can be hard to sell. Outside of the community, it is [..] usually considered as an afterthought, as something librarians and archivists do. Even within our organisations, it can be a siloed activity, and the focus is usually on our "own" collections. Thinking more broadly though, it is a global responsibility that is perhaps better described as a collaborative endeavour to ensure persistent access. It should not exist in isolation.

Torsten Reimer[1]

Il presente lavoro di ricerca (anche in considerazione della sua natura EUREKA) nasce da due principali esigenze, sia di matrice accademica sia applicativa: da un lato, vi è la necessità di una rilevazione del contesto generale, soggetto a innovazioni e progressi continui dal punto di vista normativo, di iniziative e tecnologiche, dall'altro di trarre spunto da tale ricognizione per effettuare un'analisi che proponga un confronto costruttivo e prospettive di miglioramento.

Si è visto come il contesto europeo sia caratterizzato da una molteplicità di spunti, tentativi e soluzioni: le tendenze che caratterizzano queste iniziative sono la collaborazione nel definire direzioni comuni e lo sforzo collettivo nel concretizzarle attraverso la realizzazione di strumenti a libera disposizione della comunità, che consistono sia in documenti programmatici e linee guida sia in effettivi applicativi e software.

Dal punto di vista normativo, vi è un simile intento di rendere coerenti i requisiti che determinano la qualità dei servizi di conservazione: nonostante l'assenza di un provvedimento in materia, la nuova proposta eIDAS, con l'inserimento di apposite disposizioni sui conservatori fiduciari qualificati, ha le potenzialità di rappresentare il principio di un cammino comune a livello europeo per l'uniformità delle caratteristiche per l'implementazione dei sistemi di conservazione.

Dalle realtà esaminate nel dettaglio, poi, emerge una 'fotografia' del panorama europeo sulla conservazione digitale allineata al triennio che dal termine del 2018 giunge al 2021: il

[1] *Head of Content and Research Services* presso la British Library. Citazione dalla keynote '*Does anybody care about digital preservation? Thinking about digital preservation from a perspective of access, collaboration and purpose*' (iPRES 2021, 21 ottobre 2021).

quadro descritto è composito ed evidenzia realtà che percepiscono il tema in maniera molto diversa.

L'Italia presenta una normativa piuttosto completa e frutto di significative riflessioni, che consisterà – dal primo gennaio – nelle apposite *Linee Guida sulla formazione, gestione e conservazione dei documenti informatici* emanate sulla base di quanto stabilito dal Codice per l'Amministrazione Digitale e nel *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*. Incaricata della redazione di questi documenti è l'Agenzia per l'Italia Digitale, preposta al coordinamento della strategia di digitalizzazione nazionale: a questo organo sono demandate la stesura di tali provvedimenti, le funzioni di applicazione di tali disposizioni per eseguire l'iter di accreditamento (in seguito qualificazione) e le attività di vigilanza e controllo sui soggetti, pubblici e privati, che operano con tale denominazione.

Si è evidenziato come, nonostante l'evidente qualità del corpus normativo in materia in contesto italiano, vi siano diverse criticità contenutistiche, legate al progressivo distanziamento delle autorità archivistiche dalle funzioni inerenti alla conservazione digitale e dalla definizione ancora poco chiara di alcuni requisiti e caratteristiche.

Non ultime le problematiche relative al contesto applicativo, connesse alla persistenza di una situazione ancora ibrida tra l'analogico e il digitale, al ricorso massivo all'esternalizzazione dei servizi di conservazione e all'assenza di Poli di conservazione pubblici con mandato specifico per la tenuta a lungo termine delle memorie digitali.

L'Austria, per quanto concerne la conservazione dei documenti pubblici a livello federale, mostra una gestione dei processi molto centralizzata, affidata alle competenze dell'Archivio di Stato austriaco e delle sue sedi territoriali. Pur non esistendo in normativa disposizioni specifiche in materia, l'*Österreichisches Staatsarchiv* e le autorità competenti in materia di digitalizzazione promuovono iniziative per disciplinare la tenuta a lungo termine del materiale digitale; tra queste, è stato sviluppato DigLA, sistema basato sull'architettura OAIS utilizzato per conservare la documentazione dei diversi uffici federali. Inoltre, per gestire i servizi cloud (tra cui può essere compresa in alcuni casi la conservazione), il *Bundesministerium für Digitalisierung und Wirtschaftsstandpunkt*, ha previsto la possibilità di dotarsi della certificazione *Ö-Cloud Gütesiegel*.

L'analisi del contesto francese mostra una rilevante incidenza della cultura archivistica nazionale nelle scelte normative e applicative in materia di conservazione digitale. Le disposizioni normative a questa dedicate, infatti, sono costituite da aggiornamenti del Codice del Patrimonio Culturale, che contiene dunque le indicazioni per gestire e conservare *courantes*, *intermédiaires* e *définitives* tanto analogici quanto digitali. Per quanto riguarda gli strumenti operativi, si predilige l'adozione di norme e standard internazionali, integrati da schemi nazionali, ed è attivo il progetto VITAM, che mira a fornire agli enti e alle istituzioni pubbliche un software finalizzato all'archiviazione e alla conservazione delle proprie risorse documentali digitali.

La realtà olandese rivela un contesto in aggiornamento: per quanto riguarda la normativa, la Legge archivistica sta ultimando l'iter di revisione, rinnovo e pubblicazione finalizzato all'adeguamento alle esigenze di conservazione delle memorie prodotte digitalmente. Le disposizioni sono affiancate dall'implementazione, da parte dei *Nationaal Archief*, dell'e-Depot, archivio progettato sul modello OAIS e integrato con applicativi condivisi in ambito internazionale, per la conservazione della documentazione digitale del governo olandese.

La Romania, infine, pur presentando delle disposizioni specifiche sulla documentazione elettronica, non mostra un particolare approfondimento del tema né uno sviluppo avanzato delle soluzioni tecnologiche applicate.

Dall'analisi comparata tra questi esempi, risultano interessanti differenze. Rispetto al contesto istituzionale e amministrativo, si nota un peso diverso attribuito al ruolo delle autorità archivistiche e degli organi competenti in materia di digitalizzazione in relazione al tema della conservazione digitale e alle attività ad essa legate, con la rilevazione di situazioni più definite e adeguate nei casi in cui sono preponderanti le prime.

Relativamente alle disposizioni di legge, vi sono approcci differenti rispetto alla forma, al contenuto e alla tipologia di atti vigenti: prevalente è la prassi di produrre provvedimenti redatti al fine di vincolare lo specifico ambito, in compresenza con esempi di aggiornamento della normativa primaria o di assenza di regolamentazione in materia.

Per quanto riguarda i modelli e gli standard, a sistemi centralizzati per la conservazione della documentazione digitale a lungo termine, si affiancano realtà 'distribuite', in cui si

demanda alle singole istituzioni ed enti l'implementazione dei propri ecosistemi, con soluzioni proposte da progetti nazionali, o la responsabilità di esternalizzare il servizio.

Per riassumere, volendo tracciare un quadro degli elementi positivi presenti nei casi esposti nel presente elaborato, si possono individuare diversi punti cardine per lo sviluppo di normativa, prassi e strumenti che consentano di preservare a lungo termine le memorie digitali.

È fondamentale, sia per gli aggiornamenti normativi sia per lo sviluppo di sistemi, far riferimento ai lavori collettivi svolti da organizzazioni internazionali e risultanti da iniziative promosse appositamente per l'approfondimento del tema, al fine di disporre di una visione a trecento sessanta gradi su soggetti produttori, utenti, software, hardware, architetture e processi che consenta di fronteggiare le sfide dell'obsolescenza e dell'innovazione tecnologica. È, inoltre, importante sensibilizzare al tema tutte le figure all'interno degli enti, delle istituzioni, degli organismi o di qualsiasi organizzazione privata che possano essere a diversi titolo coinvolte, per fare in modo che i professionisti della conservazione digitale abbiano il supporto formativo e finanziario adeguato a portare avanti le iniziative e a intraprendere le azioni necessarie.

In quest'ottica devono essere concepite le norme di settore: i dispositivi, per essere realmente efficaci, devono essere formulati col coinvolgimento delle autorità archivistiche e elaborati in maniera tale da prediligere sintesi e linearità, nell'ottica di ricorrere il meno possibile a provvedimenti integrativi di rango inferiore. Questo deve essere accompagnato dallo sviluppo di sistemi progettati in contesto pubblico, con la coordinazione tra istituzioni operanti in ambito archivistico e di digitalizzazione della pubblica amministrazione e che si basino su standard internazionali e applicazioni condivise, allo scopo di fornire uno strumento che consenta il deposito a lungo termine delle memorie digitali e che ne permetta la consultazione a una comunità di utenti potenzialmente illimitata.

L'elaborato si vuole concludere con delle considerazioni in prospettiva: una panoramica sulla tematica della conservazione digitale, prodotta con l'impostazione e le premesse specificate in *incipit*, implica la trattazione ad alto livello degli aspetti principali e generali. L'indagine è aperta e necessita di essere dischiusa nei suoi numerosi temi, che riguardano nello specifico i set di metadati, i formati, i sistemi di *storage*, le effettive tecnologie e i flussi

di lavoro implementati in aderenza alle norme, l'impatto dei provvedimenti settoriali in ambito civilistico, penale, fiscale, della privacy, al fine di disporre di una panoramica completa sull'argomento.

Nella consapevolezza, inoltre, che gli aggiornamenti sul tema della conservazione digitale sono costanti e incalzano a ritmo rapido e che i contesti da indagare siano molti e diversificati, sia in Europa sia nel mondo, si auspica che il presente lavoro di tesi possa costituire un punto di partenza per seguire le direzioni delle innovazioni sull'argomento e che il *range* di casi di studio descritti possa considerarsi la base per l'approfondimento di altre realtà, che fungano da ulteriore spunto di confronto e riflessione prospettica, per giungere a soluzioni che consentano di tramandare le memorie digitali per un periodo almeno tanto lungo quanto è consentito (nelle migliori condizioni) dall'analogico.

Bibliografia[1]

Aalbersberg, IJsbrand Jan – Appleton, Gabrielle – Dumontier, Michel et al, *The FAIR Guiding Principles for Scientific Data Management and Stewardship*, «Scientific Data», 3 (2016), pp.1-9, disponibile online al sito <https://doi.org/10.1038/sdata.2016.18>.

Alfier, Alessandro, *La tutela degli archivi digitali: prime esplorazioni dell'hic sunt leones?*, «Archivi», XVI, 2 (2021), Padova, Cleup, 2021, pp. 6-18.

Allegrezza, Stefano, *La certificazione dei depositi digitali: il* Data Seal of Approval, «JLIS.it Italian Journal of Library, Archives and Information Science» 6 (2015), 3, pp. 39-56, disponibile online al sito <https://www.jlis.it/article/view/11332/10624>.

–, *Verso una nuova archiveconomia: alcune riflessioni sull'evoluzione della disciplina nella transizione dall'analogico al digitale*, «JLIS.it Italian Journal of Library, Archives and Information Science», 8 (2017), 1, pp. 114-126, disponibile online al sito <https://www.jlis.it/article/view/12140/11226>.

Bailey, Jefferson – Goethals, Andrea – Ross, Roslynn – Taylor, Nicholas, *CLOUD ATLAS - Navigating the Cloud for Digital Preservation*, Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 483-485, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Blewer, Ashley – Romkey, Sarah – Spencer, Ross, *Archivematica as a Case Study for Sustained Digital Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 126-133, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Bredenberg, Karin – Lehtonen, Juha – Mosely, Sean, *Understanding and Implementing METS*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the*

[1] Per quanto riguarda le indicazioni di risorse digitali, sia in Bibliografia, sia nell'Appendice A. Siti istituzionali consultati, gli indirizzi indicati sono stati verificati alla data del 20/11/2021 e risultavano tutti attivi.

16th International Conference on Digital Preservation 2019, pp. 488-490, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Calzolaio, Simone, *Protezione dei dati personali,* in Raffaele Bifulco – Alfonso Celotto – Marco Olivetti (a cura di) *DIGESTO delle Discipline Pubblicistiche*, Milano, Wolters Kluwer Italia, 2017, pp. 594-635.

Canela, Montserrat – Deserno, Ineke – Kramer-Smyth, Jeanne, *The People And Processes of Digital Preservation- International organizations leveraging internal wisdom to build support for digital records*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 472-474, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Caplan, Priscilla, *Understanding PREMIS*, Library of Congress' Network Development and Marc Standards Office, 2009, disponibile online al sito <http://www.loc.gov/standards/premis/understanding-premis-rev2017.pdf>.

Carota, Serenella, *Dematerializzazione: la strategia della Regione Marche* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Carucci, Paola – Guercio, Maria, *Manuale di archivistica*, Roma, Carocci Editore, 2013.

Cerquetella, Luca, *Sinergie in tema di dematerializzazione tra le istituzioni della provincia di Macerata e prime esperienze concrete per la conservazione dei documenti informatici* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Ciclosi, Francesco, *Le nuove linee guida AgID e il sistema di conservazione*, «ICT Security magazine», 17 aprile 2020, disponibile online al sito <https://www.ictsecuritymagazine.com/articoli/le-nuove-linee-guida-agid-e-il-sistema-di-conservazione/#_ftn28>.

Ciuccarelli, Paolo - Mauri, Michele, *Il ruolo dell'*Information Visualization *nella progettazione di interfacce per archivi digitali eterogenei*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare,* Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale

(AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 73-88.

Collie, Aaron – Daigle Bradley J. – Davis, Corey – Tibbo, Helen –Work, Lauren, *Level up on preservation: Updating and Mapping the next generation of the Levels of Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Conrad, Mark – Engel, Felix – Garrett, John – Giaretta, David – Hughes, J. Steven – Longstreth, Terry – Zierau, Eld, *OAIS version 3 draftupdates*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 254-259, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Dappert, Angela – Bredenberg, Karin – Jefferies, Neil, *Aligning the eARK4All Archival Information Package and Oxford Common File Layout Specifications - Complementary rather than competing approaches*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 72-80, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Data retention and preservation: overview on requirements in selected countries, Ernest Young GM Limited, 2015.

Dawei, Lin – Crabtree, Jonathan - Dillo, Ingrid – Downs, Robert R. – Edmunds, Rorie - Giaretta, David, De Giusti, Marisa, et al., *The TRUST Principles for Digital Repositories*, «Scientific Data», 7 (2020), 1, pp. 1-5 disponibile online al sito <https://doi.org/10.1038/s41597-020-0486-7>.

Delneri, Francesca*, Il documento amministrativo informatico: un cammino per approssimazione. Criticità e risposte possibili, tra normativa e prassi, dalla formazione alla conservazione* «JLIS.it Italian Journal of Library, Archives and Information Science» 8 (2017), 3, pp. 26-38, disponibile online al sito <https://www.jlis.it/article/view/12193/11275>.

–, *Gli orizzonti della conservazione. Le tre età dell'archivio e il ruolo dei sistemi e degli istituti di conservazione*, «JLIS.it Italian Journal of Library, Archives and Information Science», 10 (2019), 1, pp. 11-25, disponibile online al sito <https://www.jlis.it/article/view/12433/11357>.

Dinu, Nicoleta Roxana, *Prezervarea digitala*, «Biblioteca Nationala a Romaniei. Informare si Documentare», 4 (2011), pp. 31-38, disponibile online al sito <https://www.proquest.com/docview/1437608123/fulltextPDF/7ADCB22728D4409BPQ/1?accountid=15964>.

Duranti, Luciana (a cura di), *The InterPARES project: the long-term preservation of authentic electronic records: the findings of the InterPARES Project*, 2001, disponibile online al sito <http://www.interpares.org/book/index.cfm>.

Duranti, Luciana – Preston, Randy, *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records*, Padova, Associazione Nazionale Archivistica Italiana, 2008, disponibile online al sito <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf>.

European document retention guide: a comparative view across 16 countries to help you better understand legal requirements and records management best practice, Iron Mountain, 2014.

Falcao, Patricia – Smith, Caylin– Day Thomson, Sara, *Preserving complex digital objects – Workshop*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 491-493, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Feliciati, Pierluigi*, Convergere a valle. Lo studio del punto di vista degli utenti degli ambienti culturali digitali e l'esperienza del progetto "Una Città per gli Archivi"*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare*, Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 89-112.

–, *I metadati nel ciclo di vita dell'archivio digitale e l'adozione del modello PREMIS nel contesto applicativo nazionale*, in Giorgetta Bonfiglio-Dosio - Stefano Pigliapoco (a cura di), *Formazione, gestione e conservazione degli archivi digitali. Il master FGCAD dell'Università degli Studi di Macerata*, Macerata, EUM, 2015, pp. 189-208.

–, *Gestione e conservazione di dati e metadati per gli archivi: quali standard?*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010, pp. 191-219.

Fernandes, João – Jones, Bob – Pitonnet Gaiarin, Sara – Shiers, Jamie, *ARCHIVER - Archiving and Preservation for Research Environments*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 414-416, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Foglia, Luigi – Lisi, Andrea, *Conservazione dei documenti, ecco tutte le regole nelle linee guida AgID*, «Agenda Digitale», 15 settembre 2020, disponibile online al sito <https://www.agendadigitale.eu/documenti/conservazione-dei-documenti-ecco-tutte-le-regole-nelle-linee-guida-agid/>.

Franchina, Luisa – Fumagalli, Andrea – Toccaceli, Lorenzo, *Cyber security, certificazioni e sanzioni: come prosegue l'adeguamento alle norme Ue*, «Agenda Digitale», 32 aprile 2021, disponibile online al sito <https://www.agendadigitale.eu/sicurezza/cybersecurity-certificazioni-e-sanzioni-prosegue-ladeguamento-alle-direttive-ue/>.

Franks, Patricia C. – Bernier, Anthony (a cura di) *The international directory of national archives*, , Lanham, Rowman & Littlefield, Lanham, 2018.

Fröhlich, Susanne – Schöggl-erns, Elisabeth, *Digitale Archivierung in Österreich*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 265-274, disponibile online al sito <https://journal.almamater.si/index.php/Atlanti/article/view/134/121>.

Gairey, Alan – O'Farrelly, Kevin – O'Sullivan, Jack – Smith, Richard, *A Pragmatic Application Of PREMIS - Mapping the key concepts to a real-world system*, , in Angela

Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 81-91, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Gambetta, Vincenzo, *La conservazione dei contenuti digitali; requisiti dei sistemi di* storage management, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Giaretta, David, *Advanced digital preservation*, Berlino, Springer, 2011.

Goodchild, Meghan – Hurley, Grant, *Integrating Dataverse and Archivematica for Research Data Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 234-244, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Grossi, Monica, *Gli standard per la descrizione archivistica,* in *Archivistica informatica. I documenti in ambiente digitale*, Roma, Carocci Editore, 2015, pp. 233-275.

Guercio, Maria, *Gli archivi come depositi di memorie digitali*. «DigItalia. Rivista del digitale nei beni culturali» III (2008), 2, pp. 37−52, disponibile online al sito <http://digitalia.sbn.it/article/view/280/181>.

–, *I depositi per la conservazione di archivi digitali: i requisiti di certificazione e il problema dell'autenticità*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

–, *Conservare il digitale. Principi, metodi e procedure per la conservazione a lungo termine di documenti digitali*, Roma, Editori Laterza; 2013.

–, *Archivistica informatica. I documenti in ambiente digitale*, Roma, Carocci Editore, 2015.

–, *La certificazione e i depositi digitali: il ruolo degli standard e delle linee guida*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 245-255, disponibile online al sito <https://journal.almamater.si/index.php/Atlanti/article/view/132/119>.

–, *Conservare il digitale: modello nazionale e contesto internazionale*, «DigitCult – Scientific Journal on Digital Cultures», 1 (2016), 2, pp. 19-26, disponibile online al sito <https://digitcult.lim.di.unimi.it/index.php/dc/article/view/10/10>.

–, *Conservazione, dal forum italiano un primo confronto delle normative estere*, «ForumPA Digital360», 12 Gennaio 2016 <http://www.forumpa.it/pa-digitale/documenti-conservazione-sostitutiva-pregi-e-limiti-di-un-sistema-che-non-segue-le-regole>.

–, *Depositi digitali, alla ricerca di modelli organizzativi sostenibili*, «ForumPA Digital360», 20 giugno 2016, disponibile online al sito <http://www.forumpa.it/pa-digitale/depositi-digitali-cercasi-modelli-organizzativi-sostenibili>.

–, *Archivi digitali, l'Italia li trascura: ecco i nodi irrisolti e gli obblighi disattesi*, «Agenda Digitale», 26 luglio 2018, disponibile online al sito <https://www.agendadigitale.eu/cittadinanza-digitale/archivi-digitali-litalia-li-trascura-ecco-i-nodi-irrisolti-e-gli-obblighi-disattesi/>.

Guercio, Maria – Pigliapoco, Stefano – Valacchi, Federico, *Archivi e informatica*, Lucca, Civita editoriale, 2010.

Hollander, Yvette – Steeman, Marjolein, *Preservation Metadata Dictionary - PREMIS implementation in practice*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* p. 449, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Humbert, Marion – Roussel, Stéphanie – Vasseur, Édouard, *Building the future of digital preservation in French archival services - Processes, functions and staffing for an effective digital preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 46-52, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

LaPlant, Lisa – Pennock, Maureen – Shiers, Jamie – Zuberi, Irfan, *Dawn of Digital Repository Certification Under ISO 16363 Exploring the Horizon and Beyond - Perspectives From Three Institutions*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di)

Proceedings of the 16th International Conference on Digital Preservation 2019, pp. 463-465, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Lindlar, Michelle – Rudnik, Pia, *Eye on CoreTrustSeal - Recommendations for Criterion R0 from Digital Preservation and Research Data Management Perspectives*, Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 221-233, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Lodolini, Elio, *Storia dell'archivistica italiana. Dal mondo antico alla metà del secolo XX,* Milano, Franco Angeli, 2013.

McMeekin, Sharon – Middleton, Sarah, *Engaging Decision Makers - An Executive Guide on Digital Preservation*, in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 401-433, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Mambelli, Francesca, *Una risorsa online per la storia dell'arte: il database della Fondazione Federico Zeri*, in Fabio Ciotti (a cura di) *Digital Humanities: progetti italiani ed esperienze di convergenza multidisciplinare*, Atti del convegno annuale dell'Associazione per l'Informatica Umanistica e la Cultura Digitale (AIUCD) Firenze, 13-14 dicembre 2012, Roma, Sapienza Università Editrice, 2014, pp. 113-125.

Manca, Giovanni, *Gli standard di conservazione con il regolamento eIDAS: che c'è da sapere*, «Agenda digitale», 23 gennaio 2019, disponibile online al sito <https://www.agendadigitale.eu/documenti/gli-standard-di-conservazione-con-il-regolamento-eidas-che-ce-da-sapere/>.

–, *Breve storia della PA digitale: la genesi e l'evoluzione del Codice dell'Amministrazione Digitale*, «Agenda Digitale», 6 luglio 2020, disponibile online al sito <https://www.agendadigitale.eu/cittadinanza-digitale/breve-storia-della-pa-digitale-la-genesi-e-levoluzione-del-codice-dellamministrazione-digitale/>.

–, *Conservazione digitale, la qualifica eIDAS per gli operatori: ecco come funziona*, «Agenda digitale», 09 febbraio 2021, disponibile online al sito

<https://www.agendadigitale.eu/documenti/conservazione-digitale-la-qualifica-eidas-per-gli-operatori-ecco-come-funziona/>.

–, *Nuovo regolamento eIDAS, ecco come cambia l'archiviazione elettronica*, «Agenda Digitale», 7 settembre 2021, disponibile online al sito <https://www.agendadigitale.eu/documenti/nuovo-regolamento-eidas-ecco-come-cambia-larchiviazione-elettronica/>.

Marti, Federica, *La conservazione digitale in ambito internazionale. Alcune riflessioni da ipres 2019 (Amsterdam, 16-20 settembre 2019)*, «AIDAinformazioni. Rivista di Scienze dell'Informazione», 38 (2020), 1, pp. 133-149.

Marzano, Gilberto, *Conservare il digitale,* Editrice Bibliografica, 2011.

May, Peter – Pennock, Maureen – Russo, David, *The Integrated Preservation Suite - Demonstrating a scalable preservation planning toolset for diverse digital collections,* in Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 451-452, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

–, *The Integrated Preservation Suite - Scaled and automated preservation planning for highly diverse digital collections*, Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 142-154**,** disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Mazzeo, Antonino – Nastri, Michele, *Aspetti tecnici e organizzativi della conservazione: il caso del Notariato italiano,* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Michetti, Giovanni, *Il modello OAIS,* «DigItalia. Rivista del digitale nei beni culturali», III (2008), 1, disponibile online al sito <http://digitalia.sbn.it/article/view/441/281>.

–, *Il paradosso della conservazione digitale: riflessioni sull'autenticità*, «DigItalia. Rivista del digitale nei beni culturali», V (2010), 2, disponibile online al sito <http://digitalia.sbn.it/article/view/237/148>.

–, *Lo standard UNI SInCRO: un supporto alla conservazione digitale*, «Archivi & Computer», 1 (2011), San Miniato, pp. 40-53.

Michetti, Giovanni – Prom, Chris – Pearce-Moses, Richard – Timms, Kat, *Role and meaning of arrangement and description in the digital environment,* in Luciana Duranti – Corinne Rogers, *Trusting records in the Cloud. The Creation, Management, and Preservation of Trustworthy Digital Content*, 2018, disponibile online al sito <https://www.cambridge.org/core/books/trusting-records-and-data-in-the-cloud/67BF7279744D7A1A6494994935C4DA36>.

Mustapha Mokrane, Jonas Recker, *CoreTrustSeal Certified Repositories - Enabling Findable, Accessible, Interoperable, and Reusable (FAIR) Data*, Angela Puggioni – Marcel Ras – Barbara Sierman (a cura di) *Proceedings of the 16th International Conference on Digital Preservation 2019,* pp. 92-100, disponibile online al sito <https://ipres2019.org/static/proceedings/iPRES2019.pdf>.

Pedrini, Riccardo, *In Margin of Hybrid Archives and integrated Systems*, «JLIS.it Italian Journal of Library, Archives and Information Science», 11 (2020), 3, pp. 122-135, disponibile online al sito <https://www.jlis.it/article/view/12639/11407>.

Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, Agenzia per l'Italia Digitale, disponibile online al sito <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2017-2019/doc/01_piano-triennale-per-informatica-nella-pa.html>.

Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021, Agenzia per l'Italia Digitale, disponibile online al sito <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2019-2021/index.html>.

Piano Triennale per l'Informatica nella Pubblica Amministrazione 2020-2022, Agenzia per l'Italia Digitale, disponibile online al sito <https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2020-2022/index.html>.

Pieri, Antonella – Robotti, Diego, *La tutela degli archivi digitali degli enti pubblici: un sistema ancora da progettare*, «Archivi», XIV, 2 (2019), pp. 197-203.

Pigliapoco, Stefano, *Lo standard ISO 14721 per la conservazione di contenuti digitali: prospettive di applicazione,* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

–, *La conservazione delle memorie digitali*, in Linda Giuva – Maria Guercio (a cura di) "Archivistica" , Roma, Carocci editore, 2014, pp. 287-310.

–, *Progetto archivio digitale. Metodologia, professionalità, sistemi*, Lucca, Civita editoriale, 2020.

–, *Guida alla gestione informatica dei documenti*, Lucca, Civita editoriale, 2020.

–, *Digital Preservation in Italy*: *Reflections on Models, Criteria and Solutions*, «JLIS: Italian Journal of Library, Archives and Information Science», 10 (2019), 1, pp. 1-11, <https://www.jlis.it/article/view/12521/11349>.

Pontevolpe, Gianfranco, *Gli obiettivi del Governo italiano per la dematerializzazione dei documenti,* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Popovici, Bogdan-Florin, *Electronic Records Management in Romania: More Electronic-, Less Records-Management*, «ATLANTI. Rivista di teoria e pratica archivistica moderna», 25 (2015), 1, pp. 183-192 <https://journal.almamater.si/index.php/Atlanti/article/view/126/113>.

Santoboni, Paolo, *Il percorso per la definizione di un modello di prassi archivistica per la vigilanza sugli archivi digitali*, «Archivi», XVI, 2 (2021), Padova, Cleup, 2021, pp.

Sibille, Claire, *Une nouvelle version du Référentiel général d'interopérabilité*, «Hypotheses», 11 mai 2016, disponibile al sito <https://siaf.hypotheses.org/644>.

Tommasi, Brizio Leonardo, *Project management e amministrazione digitale. Criteri di gestione e misurazione di progetti e archivi digitali*, «JLIS.it Italian Journal of Library, Archives and Information Science», 9 (2018), 3, pp. 92-108, disponibile online al sito <https://www.jlis.it/article/view/12521/11349>.

Tosoni, Luca, *Cibersecurity Act, ecco le nuove norme in arrivo su certificazione dei prodotti e servizi ICT,* «Agenda Digitale», 07 giugno 2019, disponibile online al sito

<https://www.agendadigitale.eu/sicurezza/cybersecurity-act-ecco-cosa-ci-aspetta-dopo-la-direttiva-nis/>.

Tosoni, Luca, *Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto*, «Agenda Digitale», 15 gennaio 2021, disponibile online al link <https://www.agendadigitale.eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/>.

Valacchi, Federico, *La memoria integrata nell'era digitale. Continuità archivistica e innovazione tecnologica*, Corazzano, Titivillus Edizioni, 2006.

–, «Per l'interesse della scienza e del pubblico servizio». *Una Cibrario 2.0 che riconosca agli archivi "il potere degli archivi"*, in Giorgetta Bonfiglio Dosio e Stefano Pigliapoco (a cura di) *Formazione, gestione e conservazione degli archivi digitali. Il Master FGCAD dell'Università degli Studi di Macerata*, Macerata, EUM, 2015, pp. 106-166.

Vitali, Stefano, *La conservazione a lungo termine degli archivi digitali dello Stato,* in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Vota, Ruggero, *L'opinione dei conservatori*, «Office automation. Tecnologie e modelli per il business digitale», 2 (2021), pp. 36-38, disponibile online al sito <https://www.soiel.it/sfogliabili/officeautomation/2021/febbraio-marzo/4QXjZdhY7q70qMyC.html#page=38>.

Zucchini, Alessandro, *Il Polo archivistico regionale dell'Emilia-Romagna*, in Stefano Pigliapoco (a cura di) *Conservare il digitale,* Macerata, EUM, 2010.

Appendice A. Principali siti istituzionali e ufficiali consultati[1]

Si è ritenuto utile raccogliere, in *Appendice A*, i siti istituzionali consultati per la ricostruzione del contesto di ciascuno Stato citato come caso di studio nel presente elaborato.

Austria

Piattaforma Digital Austria < https://www.digitalaustria.gv.at/>.

Portale ufficiale di consultazione della normativa austriaca <https://www.ris.bka.gv.at/default.aspx>.

Sito istituzionale del Comitato DIN <https://www.din.de/de/mitwirken/normenausschuesse/nid>.

Sito istituzionale del Ministero federale per la digitalizzazione e gli affari economici <https://www.bmdw.gv.at/>.

Sito istituzionale dell'Agenzia per la sicurezza federale tedesca (BSI) <https://www.bsi.bund.de/EN/Home/home_node.html;jsessionid=5165DC0F0E8F6928C6A7C0AA0C40EBF5.internet462>.

Sito ufficiale dell'iniziativa CoreTrustSeal <https://www.coretrustseal.org/>.

Sito ufficiale dell'iniziativa Ö-Cloud-Gütesiegel <https://oe-cloud.eurocloud.at/>.

Sito istituzionale dell'Archivio di Stato austriaco <https://www.oesta.gv.at/>.

Sito istituzionale della rete Nestor <https://www.langzeitarchivierung.de/Webs/nestor/EN/nestor/nestor_node.html>.

Francia

Portale nazionale degli Archivi di Francia <https://francearchives.fr/fr/>.

[1] Si veda la nota 1 alla Bibliografia.

Portale ufficiale di consultazione della normativa francese <https://www.legifrance.gouv.fr/>.

Sito istituzionale degli Archivi Nazionali di Francia <https://www.archives-nationales.culture.gouv.fr/fr_FR/web/guest/home>.

Sito istituzionale del progetto VITAM <https://www.programmevitam.fr/>.

Sito ufficiale dell'organismo AFNOR <https://www.afnor.org/>.

Sito istituzionale della Direzione Interministeriale Digitale <https://www.numerique.gouv.fr/>.

Internazionali (UE)

Portale Eur-LEX <https://eur-lex.europa.eu/homepage.html>.

Sito istituzionale dell'Unione Europea <https://europa.eu/european-union/index_it>.

Sito ufficiale della Digital Preservation Coalition <https://www.dpconline.org/>.

Sito ufficiale dell'European Telecommunications Standards Institute <https://www.etsi.org/about>.

Sito ufficiale dell'International Organization for Standardization <https://www.iso.org/home.html>.

Sito ufficiale dell'InterPARES project <http://www.interpares.org/>.

Sito ufficiale dell'Open Preservation Foundation <https://openpreservation.org/>.

Italia

Portale della Gazzetta Ufficiale della Repubblica Italiana <https://www.gazzettaufficiale.it/>.

Sito istituzionale del Polo Archivistico dell'Emilia Romagna <https://poloarchivistico.regione.emilia-romagna.it/>.

Sito istituzionale dell'Agenzia per l'Italia Digitale <https://www.agid.gov.it/it>.

Sito istituzionale dell'Archivio Centrale dello Stato <https://www.acs.beniculturali.it/>.

Sito istituzionale della Regione Marche < https://www.regione.marche.it/>.

Sito ufficiale della Società informatica del notariato italiano <https://www.notartel.it/notartel/index.jsp>.

Sito web di Forum PA <https://www.forumpa.it/>.

Olanda

Portale ufficiale di consultazione della normativa olandese <https://www.overheid.nl/>.

Sito istituzionale degli Archivi Nazionali d'Olanda <https://www.nationaalarchief.nl/>.

Sito istituzionale del Ministero dell'educazione, della cultura e della scienza <https://www.government.nl/ministries/ministry-of-education-culture-and-science>.

Sito istituzionale dell'Ispettorato per informazione e il patrimonio culturale <https://www.government.nl/ministries/ministry-of-education-culture-and-science>.

Sito web dell'Istituto reale olandese per la standardizzazione <https://www.nen.nl/en/>.

Sito web del Forum sulla standardizzazione < https://forumstandaardisatie.nl/>.

Romania

Portale ufficiale di consultazione della normativa rumena <http://legislatie.just.ro/>.

Sito istituzionale del Ministero delle Comunicazioni e della Società dell'Informazione della Romania <https://www.comunicatii.gov.ro/>.

Sito istituzionale dell'Archivio Nazionale della Romania <http://arhivelenationale.ro/site/?lan=0>.

Sito istituzionale dell'Autorità Rumena per la Digitalizzazione <https://www.adr.gov.ro/>.

Appendice B. Fonti normative citate

L'*Appendice B* contiene l'elenco delle norme citate per ciascun caso di studio, per il contesto italiano e per l'ambito dell'Unione Europea.

Austria

Notazione breve	Intestazione estesa
Bundesabgabenordnung – BAO	*Bundesgesetz über allgemeine Bestimmungen und das Verfahren für die von den Abgabenbehörden des Bundes, der Länder und Gemeinden verwalteten Abgaben (Bundesabgabenordnung – BAO). StF: BGBl. Nr. 194/1961*
Bundesarchivgesetz	*Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz). StF: BGBl. I Nr. 162/1999*
Bundesarchivgutverordnung	*Verordnung des Bundeskanzlers über die Kennzeichnung, Anbietung und Archivierung von Schriftgut des Bundes (Bundesarchivgutverordnung).StF: BGBl. II Nr. 367/2002*
Denkmalschutzgesetz - DMSG	*Bundesgesetz betreffend den Schutz von Denkmalen wegen ihrer geschichtlichen, künstlerischen oder sonstigen kulturellen Bedeutung (Denkmalschutzgesetz - DMSG) StF: BGBl. Nr. 533/1923*

Francia

Notazione breve	Intestazione estesa
Arrêté du 21 janvier 1988	Arrêté du 21 janvier 1988 *portant création du Conseil supérieur des archives.*
Arrêté du 17 novembre 2009	Arrêté du 17 novembre 2009 *relatif aux missions et à l'organisation de la direction générale des patrimoines*
Arrêté du 20 avril 2016	Arrêté du 20 avril 2016 *portant approbation du référentiel général d'interopérabilité*
Décret n° 2011-573	Décret n° 2011-573 du 24 mai 2011 *relatif à la partie réglementaire du code du patrimoine (Décrets en Conseil d'Etat et en conseil des ministres)*
Décret n° 2011-574	Décret n° 2011-574 du 24 mai 2011 *relatif à la partie réglementaire du code du patrimoine (livres Ier à VI)*
Décret n° 2016-1673	Décret n° 2016-1673 du 5 décembre 2016 *relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil*
Décret n° 2019-1088	Décret n° 2019-1088 du 25 octobre 2019 *relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numériqueè*
Décret n° 2020-733	Décret n° 2020-733 du 15 juin 2020 *relatif à la déconcentration des décisions administratives individuelles dans le domaine de la culture*
Ordonnance n° 2004-178	Ordonnance n° 2004-178 du 20 février 2004 *relative à la partie législative du Code du patrimoine.*
Ordonnance n° 2005-1516	Ordonnance n° 2005-1516 du 8 décembre 2005 *relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*

Ordonnance n° 2016-131	Ordonnance n° 2016-131 du 10 février 2016 *portant réforme du droit des contrats, du régime général et de la preuve des obligations*

Internazionali (UE)

Notazione breve	Intestazione estesa
Dir. 2009/24/CE	Direttiva 2009/24/CE del Parlamento Europeo e del Consiglio del 23 aprile 2009 *relativa alla tutela giuridica dei programmi per elaboratore*
Dir. UE 2015/1535	Direttiva (UE) 2015/1535 del Parlamento Europeo e del Consiglio del 9 settembre 2015 *che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*
Dir. UE 2016/1148	Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 *recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*
Reg. UE 765/2008	Regolamento (CE) n. 765/2008 del parlamento europeo e del consiglio del 9 luglio 2008 *che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti*
Reg. UE 910/2014	Regolamento (UE) 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS)*
Reg. UE 2016/679	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 (GDPR)
Reg. UE 2017/2394	Regolamento (UE) 2017/2394 del Parlamento Europeo e del Consiglio del 12 dicembre 2017 *sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e che abroga il regolamento (CE) n. 2006/2004*
Reg. UE 2018/1807	Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*
Reg. UE 2019/881	Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 *relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (Cibersecurity Act)*

Italia

Notazione breve	Intestazione estesa
Circolare n. 65/2014	Circolare N. 65 del 10 aprile 2014 *Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82*
Circolare n. 2/2018	Circolare n. 2 del 9 aprile 2018 *Criteri per la qualificazione dei Cloud Service Provider per la PA*
Circolare n. 3/2018	Circolare n. 3 del 9 aprile 2018 *Criteri per la qualificazione di servizi SaaS per il Cloud della PA*

D.L 76/2020	Decreto Legge 16 luglio 2020 n. 76 *Misure urgenti per la semplificazione e l'innovazione digitale* (Decreto Semplificazioni)
D.lgs 196/2003	Decreto Legislativo del 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali*
D.lgs 42/2004	Decreto Legislativo 22 gennaio 2004 n. 42 *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*
D.lgs 82/2005	Decreto Legislativo 7 marzo 2005 n. 82 *Codice dell'Amministrazione Digitale* (CAD)
D.lgs 235/2010	Decreto Legislativo 30 dicembre 2010, n. 235 *Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69*
D.lgs 179/2016	Decreto Legislativo 26 agosto 2016, n. 179 *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*
D.lgs 217/2017	Decreto Legislativo 13 dicembre 2017, n. 217 *Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*
DPCM 3 dicembre 2013 (C)	Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis*

	, 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005
DPCM 3 dicembre 2013 (P)	Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 *Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*
DPCM 13 novembre 2014	Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 *Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*
DPCM 2 dicembre 2019 n. 169	Decreto del Presidente del Consiglio dei Ministri 2 dicembre 2019, n. 169 *Regolamento di organizzazione del Ministero per i beni e le attività culturali e per il turismo, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance*
DPR 1409/1963	Decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 *Norme relative all'ordinamento ed al personale degli archivi di Stato*
DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* (TUDA)

Determinazione AgID n. 455/2021	Determinazione AgID n. 455 /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)*
Determinazione AgID n. 74/2021	Determinazione AgID n. 74/2021 *Revisione del "Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 e successive modificazioni"*

Olanda

Notazione breve	Intestazione estesa
AB 1995	Besluit van 15 december 1995*, houdende regelen ter uitvoering van een aantal bepalingen van de Archiefwet 1995 (Archiefbesluit)*
AW 1995	Archiefwet 1995 wet van 28 april 1995*, houdende vervanging van de Archiefwet 1962 (Stb. 313) en in verband daarmede wijziging van enige andere wetten (Archiefwet 1995)*
AW 2021	Voorstel van Wet tot intrekking van de Archiefwet 1995 *en vervanging door de Archiefwet 2021 (Archiefwet 2021)*
AR	Regeling van de Minister van Onderwijs, Cultuur en Wetenschap van 15 december 2009, nr. WJZ/178205 *(8189), met betrekking tot de duurzaamheid en de geordende en toegankelijke staat van archiefbescheiden en de bouw en inrichting van archiefruimten en archiefbewaarplaatsen (Archiefregeling)*
WOB	Wet van 31 oktober 1991*, houdende regelen betreffende de openbaarheid van bestuur (Wet openbaarheid van bestuur)*

WOO	*Voorstel van wet van de leden Snels en Van Weyenberg tot wijziging van het voorstel van wet van de leden Snels en Van Weyenberg houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid - Wijzigingswet Woo)*

Romania

Notazione breve	Intestazione estesa
Hotărâre nr. 89/2020	Hotărâre nr. 89 din 28 ianuarie 2020 *privind organizarea şi funcţionarea Autorităţii pentru Digitalizarea României*
Lege nr. 135/2007	Lege nr. 135 din 15 mai 2007 *privind arhivarea documentelor în formă electronică*
Lege nr. 138/2013	Lege nr. 138 din 30 aprilie 2013 *pentru modificarea şi completarea Legii Arhivelor Naţionale nr. 16/1996, publicată în Monitorul Oficial al României, Partea I, nr. 253 din 7 mai 2013*
Ordin nr. 489/2009	Ordin nr. 489 din 15 iunie 2009 *privind normele metodologice de autorizare a centrelor de date*
Ordin nr. 493/2009	Ordin nr. 493 din 15 iunie 2009 *privind normele tehnice şi metodologice pentru aplicarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică*
Ordin nr. 585/2011	Ordin nr. 585 din 9 mai 2011 *pentru completarea Ordinului ministrului comunicațiilor și societății informaționale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date*
Ordin nr. 1167/2011	Ordin nr. 1167 din 25 noiembrie 2011 *pentru modificarea Anexei nr. 3 la Ordinul ministrului comunicaţiilor şi societăţii informaţionale nr. 489/2009 privind normele metodologice de autorizare a centrelor de date*

Appendice C. Norme e standard citati

L'*Appendice C* contiene l'elenco degli standard citati per ciascun caso di studio, per il contesto italiano e per l'ambito internazionale.

Austria

Notazione breve	Intestazione estesa
ISO 14721:2012	*Space data and information transfer systems — Open archival information system (OAIS) — Reference model*
ISO/IEC 20000-1:2018	*Information technology — Service management — Part 1: Service management system requirements*
ISO/IEC 20000-2:2019	*Information technology — Service management — Part 2: Guidance on the application of service management systems*
ISO/IEC 27001:2013	*Information technology — Security techniques — Information security management systems — Requirements*
DIN 31644:2012-04	*Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive*

Francia

Notazione breve	Intestazione estesa
ISO 14641:2018	*Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications*
ISO 14721:2012	*Space data and information transfer systems — Open archival information system (OAIS) — Reference model*
NF 461	*Système d'archivage électronique pour compte de tiers*
NF 544	*Prestations de numérisation fidèle de documents sur support papier*

NF Z 42-013	*Archivage électronique - Recommandations et exigences*
NF Z 42-026	*Définition et spécifications des prestations de numérisation fidèle de documents et contrôle de ces prestations*
NF Z 44-022	*Modélisation des Échanges de DONnées pour l'Archivage (MEDONA)*
SEDA	*Standard d'Échange de Données pour l'Archivage*

Internazionali

Notazione breve	Intestazione estesa
CEI EN 50173-1	*Tecnologia dell'informazione — Sistemi di cablaggio strutturato. Parte 1: Requisiti generali* (citato come SR EN 50173-1 2008)
CEI EN 50173-5	*Tecnologia dell'informazione — Sistemi di cablaggio strutturato. Parte 5: Centri di elaborazione dati* (citato come SR EN 50173-5 2008)
ETSI TS 101 533-1	*Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management*
ETSI TS 102 573	*Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects*
ETSI TS 119 511	*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*
ETSI EN 319 401	*General Policy Requirements for Trust Service Providers*
ISO 9001:2015	*Quality management systems — Requirements*

ISO 14641:2018	*Electronic document management — Design and operation of an information system for the preservation of electronic documents — Specifications*
ISO 14721:2012	*Space data and information transfer systems — Open archival information system (OAIS) — Reference model*
ISO/IEC 15444-1:2019	*Information technology — JPEG 2000 image coding system — Part 1: Core coding system*
ISO 15836-1:2017	*Information and documentation — The Dublin Core metadata element set — Part 1: Core elements*
ISO 15836-2:2019	*Information and documentation — The Dublin Core metadata element set — Part 2: DCMI Properties and classes*
ISO/IEC 15408-1:2009	*Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model* (citato nella precedente versione ISO/IEC 15408-1:2005)
ISO 16363:2012	*Space data and information transfer systems — Audit and certification of trustworthy digital repositories*
ISO 16919:2014	*Space data and information transfer systems — Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*
ISO/IEC 17021-1:2015	*Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements.*
ISO/IEC 20000-1:2018	*Information technology — Service management — Part 1: Service management system requirements* (citato nella precedente versione ISO/IEC 20000-1: 2005)
ISO/IEC 20000-2:2019	*Information technology — Service management — Part 2: Guidance on the application of service management systems* (citato nella precedente versione ISO/IEC 20000-

	2: 2005 *Information technology — Service management — Part 2: Code of practice*)
ISO 20614:2017	*Information and documentation — Data exchange protocol for interoperability and preservation*
ISO 22301:2019	*Security and resilience — Business continuity management systems — Requirements*
ISO 22313:2020	*Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
ISO 23081-1:2017	*Information and documentation — Records management processes — Metadata for records — Part 1: Principles*
ISO 23081-2:2021	*Information and documentation — Metadata for managing records — Part 2: Conceptual and implementation issues* (citato anche nella precedente versione ISO 23081-2:2016)
ISO/IEC 27001:2013	*Information technology — Security techniques — Information security management systems — Requirements* (citato anche nella precedente versione ISO/IEC 27001: 2006)
ISO/IEC 27002:2013	*Information technology — Security techniques — Code of practice for information security controls* (citato anche nella precedente versione ISO/IEC 17799: 2006)
ISO 37001:2016	*Anti-bribery management systems — Requirements with guidance for use*
TIA/EIA 942 2005	*Telecommunications Infrastructure Standard for Data Centers*

Italia

Notazione breve	Intestazione estesa
ETSI EN 319 401	*General Policy Requirements for Trust Service Providers*

ETSI TS 101 533-1	*Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management*
ETSI TS 119 511	*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*
ISO 9001:2015	*Quality management systems — Requirements*
ISO 14721:2012	*Space data and information transfer systems — Open archival information system (OAIS) — Reference model*
ISO 16363:2012	*Space data and information transfer systems — Audit and certification of trustworthy digital repositories*
ISO 22313:2020	*Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
ISO 37001:2016	*Anti-bribery management systems — Requirements with guidance for use*
UNI 11386:2020	*Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SiNCRO)*

Olanda

Notazione breve	Intestazione estesa
BIR 2012	*Baseline Informatiebeveiliging Rijksdienst. Tactisch Normenkader (TNK)*
ISO 14721:2012	*Space data and information transfer systems — Open archival information system (OAIS) — Reference model*
ISO 23081-1:2017	*Information and documentation — Records management processes — Metadata for records — Part 1: Principles*
ISO 23081-2:2021	*Information and documentation — Metadata for managing records — Part 2: Conceptual and*

	implementation issues (citato nella precedente versione ISO 23081-2:2016)
ISO/IEC 27001:2013	*Information technology — Security techniques — Information security management systems — Requirements*
ISO/IEC 27002:2013	*Information technology — Security techniques — Code of practice for information security controls*

Romania

Notazione breve	Intestazione estesa
ISO/IEC 15408-1:2009	*Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model* (citato nella precedente versione ISO/IEC 15408-1:2005)
ISO/IEC 20000-1:2018	*Information technology — Service management — Part 1: Service management system requirements* (citato nella precedente versione ISO/IEC 20000-1: 2005)
ISO/IEC 20000-2:2019	*Information technology — Service management — Part 2: Guidance on the application of service management systems* (citato nella precedente versione ISO/IEC 20000-2: 2005 *Information technology — Service management — Part 2: Code of practice*)
ISO 20614:2017	*Information and documentation — Data exchange protocol for interoperability and preservation*
ISO/IEC 27001:2013	*Information technology — Security techniques — Information security management systems — Requirements* (citato nella precedente versione ISO/IEC 27001: 2006)

ISO/IEC 27002:2013	*Information technology — Security techniques — Code of practice for information security controls* (citato anche nella precedente versione ISO/IEC 17799: 2006)
CEI EN 50173-1	*Tecnologia dell'informazione — Sistemi di cablaggio strutturato. Parte 1: Requisiti generali* (citato come SR EN 50173-1 2008)
CEI EN 50173-5	*Tecnologia dell'informazione — Sistemi di cablaggio strutturato. Parte 5: Centri di elaborazione dati* (citato come SR EN 50173-5 2008)
TIA/EIA 942 2005	*Telecommunications Infrastructure Standard for Data Centers*