ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

SAF • SCUOLA DI ALTA FORMAZIONE

Dematerializzazione documentale: temi per la consulenza.
Prima parte.
Conservazione digitale. Evoluzione del quadro normativo

nr. 66. Commissione Informatica CCIAA e Registro Imprese di Milano

a cura di: Pietro Luca Agostini, Ruggiero Delvecchio, Davide Grassano, Giuseppe Mantese, Francesco Milano

i quaderni

S.A.F. LUIGI MARTINO
Fondazione dei Dottori Commercialisti di Milano

Dematerializzazione documentale: temi per la consulenza.
Prima parte.

Conservazione digitale. Evoluzione del quadro normativo

nr. 66. Commissione Informatica CCIAA e Registro Imprese di Milano

a cura di
Pietro Luca Agostini, Ruggiero Delvecchio, Davide Grassano, Giuseppe Mantese, Francesco Milano

I Quaderni della Scuola di Alta Formazione

Direttore Responsabile:

Patrizia Riva

Segreteria:

Elena Cattaneo
corso Europa, 11 • 20122 Milano
tel: 02 77731121 • fax: 02 77731173

Autorizzazione del Tribunale di Milano al n° 765 del 11 dicembre 2006 • R.O.C. n. 16851

INDICE

Presentazione 5

1. La "conservazione digitale a norma": inquadramento sistematico e approfondimenti applicativi 9

   Premessa: normativa e prassi interpretativa commentate 9
   Introduzione: il concetto di "conservazione digitale a norma" 12
   Le caratteristiche del sistema di conservazione 15
   Modelli organizzativi, ruoli, funzioni e responsabilità nei processi di conservazione 18
   Il processo di conservazione 24
   Il manuale di conservazione 27
   Ricapitolazione: una visione d'assieme 30
   Approfondimento I: il responsabile della conservazione 32
   Approfondimento II: aspetti contrattualistici 41

2. Sicurezza e continuità operativa del sistema di conservazione 49

   Il quadro normativo di riferimento 49
   Sicurezza per la gestione dei dati personali 51
   Sicurezza nell'ambito di transazioni elettroniche 52
   Sicurezza dei documenti classificati 53
   Regole Tecniche per la gestione e la sicurezza dei sistemi di conservazione e standard di riferimento 53
   Manuale di conservazione e sicurezza dei dati 59
   Rischi e minacce riguardanti un Sistema di Conservazione 60
   Il Framework Nazionale di cyber security 63

3. Conservazione digitale in campo contabile e tributario 69

   Introduzione 69

Il D.M.E.F. 17/06/2014: conservazione digitale a norma in ambito tributario 71
Regole tecniche di conservazione digitale a norma 75
Il responsabile della conservazione 76

4. La tenuta della contabilità e la conservazione dei documenti contabili e fiscali all'estero 77

Premessa 77
I documenti presi in esame 77
I sistemi gestionali internazionali 78
Il quadro normativo di riferimento 79
Evoluzione Storica dell'Art. 39 del D.P. R. 633/1972 82
Alcune considerazioni 84
La conservazione elettronica delle fatture emesse in formato elettronico, dei registri e degli altri documenti così come previsto dall'art. 39 DPR 633/1972 85
La conservazione elettronica nei paesi in cui esista uno strumento giuridico che disciplini la reciproca assistenza 88
Considerazioni finali 89

5. Il Regolamento eIDAS: scenari e indicazioni operative 91

Oggetto e ambito di applicazione 91
Entrata in vigore del regolamento 92
Il regolamento in dettaglio 95
Identificazione elettronica 95
I Servizi fiduciari: quale perimetro 101
Firme elettroniche 102
Il sigillo elettronico 106
Altri servizi fiduciari 108
Effetti giuridici dei documenti elettronici 109
Il Regolamento eIDAS e gli impatti sul Codice dell'Amministrazione digitale 110
Il Regolamento eIDAS e lo SPID 111

PRESENTAZIONE[*]

La Commissione Informatica dell'Ordine di Milano ha da sempre seguito molto da vicino e con grande attenzione l'evoluzione della "dematerializzazione documentale", locuzione che vuole sinteticamente evocare l'idea di poter sostituire il supporto digitale a quello cartaceo nella gestione dei documenti, preservandone comunque la piena validità giuridica.

Si tratta di materia trasversale e strategica, che coinvolge tutti i settori aziendali, pubblici e privati, e, sempre più pervasivamente anche il singolo cittadino. A livello sovranazionale e nazionale la dematerializzazione è considerata una delle leve più potenti e promettenti per un importante recupero di efficienza, attraverso la drastica riduzione dello *administrative burden*, e di efficacia, grazie al miglioramento della qualità, dell'accessibilità e della fruibilità dei contenuti documentali.

L'importanza della materia ha indotto la Commissione, ormai diversi anni fa, a costituire uno specifico Gruppo di Lavoro, peraltro disponendo nel proprio organico di Colleghi che fin dall'esordio, tra i primissimi, hanno studiato il fenomeno, hanno pubblicato i risultati della loro ricerca, hanno prodotto una intensa e costante attività formativa per la S.A.F., hanno accumulato esperienza operativa applicativa nel partecipare a progetti di non secondaria rilevanza. A questi, nel tempo, si sono aggiunti, con entusiasmo, vista l'attualità e la prevedibile evoluzione della materia, anche i più giovani.

La costante fluidità ed espansione multidirezionale, del tutto fisiologica, del quadro normativo e degli scenari tecnologici di riferimento, oltretutto in una materia tipicamente interdisciplinare, ha sempre reso estremamente difficile consolidare in pubblicazioni unitarie compendi

---

[*] A cura di Mauro Coazzoli, Dottore Commercialista, Revisore Legale e Pubblicista, Presidente Commissione Informatica CCIAA e Registro Imprese di Milano.

sistematici ed esaustivi, che potessero durare, nella loro attualità, più di qualche mese. Questo è il motivo per cui gli articoli qui raccolti sono quasi privi di riferimenti bibliografici, compresi quelli relativi agli Autori stessi, e, per lo stesso motivo, il Quaderno assume, se vogliamo, maggior valore.

Scartata pertanto l'idea di creare un compendio sul "come fare", peraltro di brevissima longevità e necessariamente caratterizzato da approssimazioni dottrinali che non si sono ritenute sostenibili, ci si è piuttosto interrogati, sulla base dell'esperienza consulenziale maturata in anni di attività sul campo, sul "cosa ci viene chiesto", con maggiore costanza, nella nostra veste professionale, che richiede sì risposte applicative, ma fornite sulla base di riflessioni e approfondimenti che conducano a scelte ragionate, spesso da condividere con la committenza e con i vincoli, economici, organizzativi, giuridici, ad essa propri.

Nel fare questo, si è al contempo cercato di esplorare un *range* di argomenti costruito sistematicamente e sufficientemente completo.

Da tale confronto, è emersa una selezione di temi che, nell'insieme, vanno a costituire quella che si ritiene essere una buona base di riferimento, peraltro di più lunga longevità, per il Collega coinvolto in scelte e pareri connessi con la materia:

- conservazione digitale a norma, nel Codice dell'Amministrazione Digitale e nelle relative regole tecniche (ma anche declinata nel settore contabile-tributario, con una ulteriore specificazione rispetto alla conservazione all'estero), completata da una focalizzazione su un tema molto sentito dagli operatori, quello della sicurezza;
- fatturazione elettronica nei suoi argomenti ancora non del tutto focalizzati, FEPA (fatturazione elettronica verso la P.A.) e sua gestione da parte dello Studio;
- l'evoluzione prossima del quadro normativo, con una attenta disamina del Regolamento eIDAS;
- infine, con il contributo da parte di Autori, che sentitamente ringraziamo, che in ruoli primari gestiscono la ricerca presso gli Osservatori del POLIMI di più attinente focalizzazione, e che già hanno partecipato anche alla formazione della S.A.F., un tentativo di risposta, basato sui risultati della ricerca scientifica, alle domande che ci vengono poste, anche nella nostra veste di esperti di organizzazione aziendale, sugli scenari futuri, sia di sistema, che per la Professione.

Pur essendosi posti l'obiettivo di tentare di conferire spessore dottrinale e scientifico a quanto trattato, non ci si è certo dimenticati dell'istanza applicativa, per cui gli articoli, ove consigliabile o possibile, sono stati corredati da riepiloghi, individuazione di punti di attenzione,

check-list, o approfondimenti di diretto supporto alla soluzione dei non facili problemi del "come fare".

Mi auguro che questo lavoro intellettuale possa essere per tutti i Colleghi di utile stimolo e pratico utilizzo nella complessa vita dello Studio del professionista moderno.

1. LA "CONSERVAZIONE DIGITALE A NORMA": INQUADRAMENTO SISTEMATICO E APPROFONDIMENTI APPLICATIVI[*]

Premessa: normativa e prassi interpretativa commentate

Il quadro normativo di riferimento per la c.d. dematerializzazione di documenti aventi rilevanza giuridica è negli anni stato caratterizzato da una notevole fluidità, nonché da una progressiva espansione che ha seguito un trend sempre crescente.

La normativa, che potremmo definire di carattere generale, di applicazione sia al settore pubblico che a quello privato, è stata, nel 2005, accorpata nel Codice dell'Amministrazione Digitale (CAD), D.Lgs. 82/2005, il quale tuttavia, successivamente alla sua emanazione, ha subito diverse modificazioni integrazioni, tutt'altro che secondarie.

A sua volta, il CAD effettua costantemente rinvii di dettaglio alle c.d. regole tecniche, emanate, per le diverse materie che vanno a disciplinare (firme elettroniche, validazione temporale, formazione del documento, protocollo, conservazione, etc.), secondo le modalità previste dall'art. 71. Anche le regole tecniche hanno subito nel tempo diversi e sostanziali mutamenti.

L'espansione del quadro normativo è inoltre dovuta all'inserimento degli istituti della dematerializzazione nei diversi contesti di applicazione della stessa, spesso regolati da normativa (in senso lato) speciale, ad esempio in campo amministrativo, tributario, assicurativo, lavoristico, etc.

Da ultimo, il rapporto con la normativa dell'Unione, dapprima sostanzialmente limitato, per quanto qui di interesse, alla direttiva 1999/93/CE o alle direttive sulla fatturazione elettronica, si è fatto

---

[*] A cura di Pietro Luca Agostini, Dottore Commercialista e Revisore Legale, Coordinatore Gruppo di Lavoro "Dematerializzazione documentale", Commissione Informatica CCIAA e Registro Imprese di Milano ODCEC Milano.

necessariamente più stringente, a seguito dell'emanazione del Regolamento eIDAS,[1] che entra in vigore il 1 luglio 2016.

Vengono qui di seguito indicati in grassetto gli estremi abbreviati mediante i quali i riferimenti normativi o di prassi, elencati in ordine di rilevanza, citati più frequentemente o commentati con maggiore approfondimento nell'articolo vengono richiamati nel testo.

CAD – Codice dell'amministrazione digitale - Decreto legislativo del 7 marzo 2005, n. 82.

d.p.c.m. 3 dicembre 2013 (conservazione) – 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.

Deliberazione Cnipa n. 11/2004 – Centro Nazionale per l'Informatica nella Pubblica Amministrazione - Deliberazione 19 febbraio 2004, Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Articolo 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Linee guida AgID – Agenzia per l'Italia Digitale – Presidenza del Consiglio dei Ministri, Linee guida sulla conservazione dei documenti informatici, Versione 1.0 – dicembre 2015.

d.p.c.m. 3 dicembre 2013 (protocollo) – 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 al D.Lgs. n. 82 del 2005.[2]

d.p.c.m. 13 novembre 2014 – decreto del Presidente del Consiglio dei Ministri, 13 novembre 2014, Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e

---

[1] Al Regolamento eIDAS e al suo impatto anche sull'ordinamento giuridico nazionale è dedicato un apposito articolo del presente Quaderno.

[2] Nota bene: i due d.p.c.m. del 3 dicembre 2013 non devono essere confusi. Quando nel testo si cita il d.p.c.m. 3 dicembre 2013, salvo diversa indicazione, il riferimento è al d.p.c.m. che contiene le regole tecniche in materia di sistemi di conservazione. I due d.p.c.m. del 3 dicembre 2013 e il d.p.c.m. 13 novembre 2014 condividono i medesimi allegati.

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.

d.m.e.f. 17 giugno 2014 – Ministero dell'Economia e della Finanze, decreto 17 giugno 2014, Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.

d.p.c.m. 22 febbraio 2013 – decreto del Presidente del Consiglio dei Ministri, 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4,28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del D.Lgs. n. 82 del 2005.

d.p.r. 445/2000 – decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

D.Lgs. 70/2003 – decreto legislativo 9 aprile 2003, n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

D.Lgs. 196/2003 – decreto legislativo del 30/06/2003 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.

Circolare 36E/2006 – Agenzia delle Entrate, Direzione Centrale Normativa e Contenzioso, Circolare del 06/12/2006 n. 36 - Oggetto: Decreto ministeriale 23 gennaio 2004 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto.

Direttiva 1999/93/CE – direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche.

Regolamento eIDAS – Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio, 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.

Nell'articolo viene esaminato sistematicamente il quadro di riferimento generale per la conservazione digitale norma, fondamentalmente

costituito dal CAD, dal d.p.c.m. 3 dicembre 2013 e, per il suo residuale valore, dalla Deliberazione Cnipa n. 11/2004. Quanto esposto viene quindi riepilogato in un paragrafo riassuntivo, per fornisce una visione d'assieme di quanto esaminato in dettaglio.

L'articolo viene chiuso da due approfondimenti su tematiche di estremo rilievo dal punto di vista applicativo e che possono coinvolgere direttamente le competenze dei Commercialisti: le problematiche connesse al ruolo del responsabile della conservazione e gli aspetti contrattualistici dell'affidamento in *outsourcing* della conservazione.

Introduzione: il concetto di "conservazione digitale a norma"

La funzione primaria della c.d. "conservazione digitale a norma" (in passato già denominata anche "conservazione sostitutiva"[3]) è quella di garantire nel tempo la validità giuridica dei documenti informatici, sia nativi, vale a dire formatisi sin dall'origine su supporto elettronico, sia generati tramite la digitalizzazione di documenti originali analogici (generalmente cartacei).

Il concetto viene esplicitato con estrema chiarezza all'art. 43 (Riproduzione e conservazione dei documenti), comma 1, del CAD:

"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

[3] La locuzione è caduta in disuso nell'errata convinzione che evocasse la sola sostituzione di un documento informatico ad un documento cartaceo (o analogico) già esistente. In effetti, la locuzione voleva anche significare che, nel caso il documento fosse nativo informatico, questo potesse sostituire il documento cartaceo che altrimenti sarebbe stato obbligatorio stampare. In quest'ottica, la c.d. terminazione del procedimento di conservazione sostitutiva di un documento informatico coincideva concettualmente con la stampa del documento cartaceo, vale a dire col momento in cui il documento veniva ad esistenza, oppure col momento a partire dal quale il documento originale cartaceo avrebbe potuto essere distrutto. Il concetto secondo il quale un documento informatico venisse ad esistenza solo grazie alla terminazione o chiusura del processo di conservazione è stato per molto tempo il principio cardine del nostro ordinamento in tema di dematerializzazione. Tale principio è in fase di progressivo abbandono e, da ultimo, il tema viene rimodellato dal combinato disposto dei due d.p.c.m. del 3 dicembre 2013 e del d.p.c.m. 13 novembre 2014, introducendo, sostanzialmente, nella dematerializzazione documentale i tradizionali concetti archivistici di "archivio corrente", di "archivio di deposito" e di "archivio storico".

rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71".

Risulta poi evidente che, oltre a dover essere correttamente conservato, il documento informatico deve essersi correttamente formato, vale a dire conformemente a quanto stabilito dal CAD, dalle relative regole tecniche e dalla eventuale normativa speciale applicabili.[4]

In altri termini, l'intero ciclo di vita del documento informatico, dalla sua formazione alla sua distruzione (c.d. scarto) deve essere conforme alla normativa in tema di dematerializzazione.

Nell'articolo ci si occupa degli aspetti che riguardano la conservazione digitale, fase del ciclo di vita del documento informatico che inizia con il "Trasferimento nel sistema di conservazione" (si vedano gli artt. 7 e 11 del d.p.c.m. 13 novembre 2014).

Si consideri, infatti, che è la normativa stessa,[5] come si vedrà meglio anche in seguito, che scinde il ciclo di vita del documento in due macro-fasi, quella della gestione documentale e quella della conservazione, ponendo a tal fine alcuni principi fondamentali:

- il sistema di gestione documentale deve essere logicamente distinto dal sistema di conservazione;
- il sistema di gestione documentale è governato (nella P.A.) dal responsabile della gestione documentale, mentre il sistema di conservazione è governato dal responsabile della conservazione, ancorché i due ruoli, che restano comunque distinti, possano essere accorpati in un'unica persona;

---

[4] Questo, dal punto di vista della dematerializzazione; qui non ci si sta occupando della correttezza del procedimento, ad esempio amministrativo, che ha portato alla formazione del documento.

[5] Cfr. anche Linee guida AgID p. 81: "La normativa italiana infatti ha da sempre differenziato il sistema di conservazione dal servizio di gestione documentale in quanto identificano fasi differenti della vita di un archivio:

- il servizio di gestione documentale permette la gestione dell'archivio corrente ovvero dei documenti utili alla trattazione dei procedimenti e degli affari in corso
- il sistema di conservazione garantisce, nel lungo termine, il valore legale dei documenti conservati e l'esibizione all'utente che rientrando nella "comunità di riferimento" ha diritto alla consultazione dei documenti conservati."

• il passaggio di consegne del documento informatico da una sfera di responsabilità all'altra è tracciato da un "rapporto di versamento" dei contenuti informativi nel sistema di conservazione avente esito positivo (col significato giuridico di "presa in carico" da parte del responsabile della conservazione), rapporto che, nella P.A., deve essere controllato dal responsabile della gestione documentale.

Il tema della conservazione digitale a norma viene qui trattato nei suoi caratteri di applicazione generale, vale a dire come delineato nel CAD e nelle specifiche regole tecniche (d.p.c.m. 3 dicembre 2013). Il significato di descriverne sistematicamente gli elementi essenziali deriva dai notevoli cambiamenti che il d.p.c.m. 3 dicembre 2013 ha apportato rispetto alle precedenti regole tecniche, vale a dire la Deliberazione Cnipa n. 11/2004, andando a modificare in modo profondo processi e relativi assetti organizzativi in uso da circa un decennio e ai quali gli operatori erano ormai assuefatti.[6] La "nuova" conservazione digitale a norma si basa su un impianto normativo più complesso e articolato che in passato (il d.p.c.m. 3 dicembre 2013 è corredato da cinque allegati tecnici) e che presenta nodi interpretativi non ancora del tutto sciolti.

Come per le precedenti regole tecniche, è opportuno sottolineare che il quadro delineato dal d.p.c.m. 3 dicembre 2013 è di riferimento e applicazione generale, ma può subire alcune varianti in relazione alla sua

---

[6] Il d.p.c.m. 3 dicembre 2013 è entrato in vigore l'11 aprile 2014. La progressiva sostituzione della Deliberazione Cnipa n. 11/2004 avviene ai sensi dell'art. 14 (Disposizioni finali) del d.p.c.m. stesso:

"1. Il presente decreto entra in vigore il trentesimo giorno successivo alla data di pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

2. I sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del presente decreto secondo un piano dettagliato allegato al manuale di conservazione. Fino al completamento di tale processo per tali sistemi possono essere applicate le previgenti regole tecniche. Decorso tale termine si applicano in ogni caso le regole tecniche di cui al presente decreto.

3. Fino al completamento del processo di cui al comma 2, restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti.

4. La deliberazione CNIPA n. 11/2004 cessa progressivamente di avere efficacia nei termini previsti dall'art. 14 (Disposizioni finali) del d.p.c.m. 3 dicembre 2013."

declinazione nella normativa speciale applicabile a specifici settori, ad esempio, in quello tributario, ad opera del d.m.e.f. 17 giugno 2014.[7]

Le caratteristiche del sistema di conservazione

Perché la conservazione digitale possa essere considerata "a norma", innanzitutto dovrà essere rispettato il disposto dell'art. 44 (Requisiti per la conservazione dei documenti informatici) del CAD, il che ci fa spostare il focus sulle caratteristiche funzionali che necessariamente deve presentare il sistema di conservazione utilizzato.

Infatti, l'art. 44 stabilisce quanto segue:

"1. Il sistema di conservazione dei documenti informatici assicura:

– 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;

– l'integrità del documento;

– la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

– 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."

"1-*bis*. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza."

"1-*ter*. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito

[7] Il d.m.e.f. 17 giugno 2014 viene esaminato in altro articolo del presente Quaderno.

dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche."

I suddetti principi, stabiliti in termini generali dall'art. 44 del CAD, vengono poi corredati dei necessari dettagli per una loro corretta applicazione operativa tramite il d.p.c.m. 3 dicembre 2013, in particolare, per quanto qui in via introduttiva trattato, all'art. 3 (Sistema di conservazione):

"1. In attuazione di quanto previsto dall'art. 44, comma 1, del Codice, il sistema di conservazione assicura, dalla presa in carico dal produttore di cui all'art. 6 fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati di cui all'allegato 5 al presente decreto;

b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati di cui all'allegato 5 al presente decreto, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

2. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.

3. Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

4. Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il sistema di conservazione sono riportati negli allegati 2 e 3 al presente decreto."

A questo punto, è opportuno porre in evidenza che il d.p.c.m. 3 dicembre 2013 ha adottato come termine di riferimento il modello OAIS (Open Archival Information System) - ISO 14721:2002.[8]

[8] Successivamente, lo standard è stato aggiornato e denominato ISO 14721:2012. E' opportuno precisare che il modello OAIS, dal punto di vista informatico, non è un modello di *design*, quanto piuttosto un modello concettuale-organizzativo.

Il modello OAIS, oltre a voler delineare, come si evince dalla sua stessa denominazione, un sistema "aperto", vale a dire accessibile a *community* di utenti opportunamente profilate (anche nella limitazione del diritto di accesso stesso), si pone come riferimento anche per la c.d. *long term preservation*, una conservazione sicura di lungo termine, che tenga conto anche dell'interoperabilità nell'acquisizione e nello scambio delle informazioni e dei documenti.

Conseguentemente a questa impostazione, le regole tecniche, all'art. 4 (Oggetti della conservazione) del d.p.c.m. 3 dicembre 2013 impongono ulteriori requisiti che devono essere obbligatoriamente rispettati nell'implementazione e nel funzionamento del sistema di conservazione:

"1. Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

a) pacchetti di versamento;
b) pacchetti di archiviazione;
c) pacchetti di distribuzione.

2. Ai fini dell'interoperabilità tra i sistemi di conservazione, i soggetti che svolgono attività di conservazione dei documenti informatici adottano le specifiche della struttura dati contenute nell'allegato 4, almeno per la gestione dei pacchetti di archiviazione."

La particolare terminologia utilizzata richiede alcuni chiarimenti di tipo definitorio (si veda anche l'Allegato 1 al d.p.c.m. 3 dicembre 2013):

– un pacchetto informativo è un "contenitore" digitalizzato che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare (che potrebbero anche essere analogici);

– il pacchetto di versamento (PdV) è il pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione; in altri termini, il PdV è lo strumento mediante il quale i documenti informatici e i relativi metadati (o anche solo i metadati, per modificarne/integrarne dei precedenti ovvero perché i documenti sono analogici) vengono inviati al sistema di conservazione;

– il pacchetto di archiviazione (PdA) è un pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del d.p.c.m. 3 dicembre 2013 e secondo le modalità riportate nel manuale di conservazione;

– il pacchetto di distribuzione (PdD) è un pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua

richiesta.

Almeno il PdA, in via obbligatoria, deve essere rispondente anche a precise disposizioni normative contenute appunto nell'Allegato 4 denominato "Specifiche tecniche del pacchetto di archiviazione", che illustra la struttura descrittiva dell'indice del pacchetto di archiviazione (IPdA).

Tale struttura, a sua volta, è configurata facendo riferimento allo standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010), il quale costituisce lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione.

Modelli organizzativi, ruoli, funzioni e responsabilità nei processi di conservazione

Ai sensi dell'art. 5, comma 1, del d.p.c.m. 3 dicembre 2013:

– il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti;

– tali modelli devono garantire la distinzione logica tra il sistema di conservazione e il sistema di gestione documentale, se esistente.

I modelli organizzativi di riferimento, ai sensi del combinato disposto dell'art. 44, in particolare al comma 1-*ter*, del CAD e dell'art. 5, comma 2, del d.p.c.m. 3 dicembre 2013, prevedono che la conservazione possa essere svolta:

a) all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare;

b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia Digitale.

Pertanto, sinteticamente, la conservazione può essere gestita mediante soluzioni *in-house* oppure in *outsourcing*, totale o parziale.

Si noti che l'*outsourcer* può essere sia un soggetto pubblico che un soggetto privato, ma che, in ogni caso, deve essere in grado di gestire il servizio disponendo di idonee strutture organizzative e tecnologiche.

Anche le Pubbliche Amministrazioni possono gestire la conservazione al proprio interno, ma se optano per la soluzione in *outsourcing* devono obbligatoriamente, ai sensi dell'art. 5, comma 3, del d.p.c.m. 3 dicembre 2013, affidare i processi di conservazione a conservatori accreditati presso l'Agenzia per l'Italia Digitale (AgID), ai sensi dell'art. 44-*bis*, comma 1, del

CAD.

Un "conservatore accreditato" è un soggetto che, mediante idonea procedura amministrativa, ha conseguito il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza; inoltre il conservatore accreditato è soggetto al costante controllo e monitoraggio - mediante ispezioni periodiche, richieste di documentazione, invio del rapporto quadrimestrale, etc. - da parte dell'AgID nell'esplicazione della propria attività istituzionale di vigilanza.

Ai sensi dell'art. 6, comma 7, del d.p.c.m. 3 dicembre 2013, la conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all'art. 5, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.

Ai sensi del successivo comma 8, il soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal D.Lgs. 196/2003.

I ruoli e le responsabilità fondamentali in un sistema di conservazione vengono individuati dall'art. 6 del d.p.c.m. 3 dicembre 2013 e sono i seguenti:

- produttore;
- utente;
- responsabile della conservazione.

I ruoli di produttore e utente sono sostanzialmente tratti dal modello OAIS.

Il produttore è una persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il PdV ed è responsabile della trasmissione del suo contenuto al sistema di conservazione.

Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.

Più in dettaglio, ai sensi dell'art. 6 comma 3, del d.p.c.m. 3 dicembre 2013, "il responsabile della gestione documentale o il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi assicura la trasmissione del contenuto del pacchetto di versamento, da lui prodotto, al sistema di conservazione secondo le modalità operative definite nel manuale di conservazione".

L'utente può essere una persona, un ente o un sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse. Nel modello OAIS, gli utenti,

tipicamente, vengono raggruppati in *community*, diversificate per esigenze informative, diritti di accesso alle informazioni, etc.

L'utente è quindi il destinatario dei PdD.

A seconda del modello organizzativo adottato, produttore e utente potranno essere interni o esterni al sistema di conservazione (art. 6, comma 2, d.p.c.m. 3 dicembre 2013).

Il responsabile della conservazione, ruolo determinato nei suoi profili giuridici e funzionali dalla normativa nazionale, definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia, in relazione al modello organizzativo adottato ai sensi dell'art. 5.

Il responsabile della conservazione è, nel contesto normativo, figura-chiave rispetto al sistema di conservazione; infatti le sue funzioni vengono dettagliatamente descritte in apposito articolo (art. 7 - Responsabile della conservazione) del d.p.c.m. 3 dicembre 2013.

Il comma 1 prevede quanto segue.

"1. Il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice, oltre che con il responsabile della gestione documentale ovvero con il coordinatore della gestione documentale ove nominato, per quanto attiene alle pubbliche amministrazioni. In particolare il responsabile della conservazione:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale

degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

j) assicura 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;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede, 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;

m) predispone il manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti."

I commi 3 e 4 prevedono che nelle pubbliche amministrazioni il ruolo del responsabile della conservazione sia svolto da un dirigente o da un funzionario formalmente designato ovvero che il ruolo possa essere svolto dal responsabile della gestione documentale ovvero dal coordinatore della gestione documentale, ove nominato.

Quindi, come già anticipato, i ruoli restano due, ma, anche per esigenze organizzative o in base alla disponibilità di risorse, possano essere ricoperti dalla stessa persona.

Appare opportuno immediatamente precisare che non è necessario che il responsabile della conservazione disponga direttamente di tutte le competenze, le strutture o le abilità necessarie per gestire il processo di conservazione.

Infatti, ai sensi del comma 6 dell'art. 6 del d.p.c.m. 3 dicembre 2013, "il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato."

Inoltre, i conservatori accreditati presso AgID, devono individuare e

nominare, nell'ambito della propria sfera giuridico-organizzativa, le figure munite dei necessari profili professionali per ricoprire i ruoli seguenti, essendo, anche in questo caso, comunque ammessa la possibilità che la stessa persona possa assumere più ruoli. Qui di seguito, per ogni ruolo vengono riportate tra parentesi le attività associate allo stesso.

– Ruolo: Responsabile del servizio di conservazione (Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; - definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; - corretta erogazione del servizio di conservazione all'ente produttore; - gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.)

– Ruolo: Responsabile della funzione archivistica di conservazione (Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.)

– Ruolo: Responsabile del trattamento dei dati personali (Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; - garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.)

– Ruolo: Responsabile della sicurezza dei sistemi per la conservazione (Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.)

– Ruolo: Responsabile dei sistemi informativi per la conservazione (Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; - monitoraggio del mantenimento dei livelli di servizio

(SLA) concordati con l'ente produttore; - segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; - pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; - controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.)

– Ruolo: Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; - pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; - monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; - interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.)

Per quanto la presenza dei sopraelencati ruoli sia obbligatoria solo per i conservatori accreditati, i quali, tra l'altro, potrebbero dover gestire l'erogazione del servizio verso un numero anche molto elevato di produttori /utenti, una attenta disamina delle funzioni necessarie, e quindi delle relative competenze e strutture organizzative, è elemento fondamentale per orientare l'eventuale scelta tra soluzioni *in-house* e soluzioni in *outsourcing*.

Si deve anche tenere presente che le pubbliche amministrazioni che optano per l'*outsourcing*, come già ricordato, devono obbligatoriamente affidarsi a conservatori accreditati, per cui, indirettamente, il legislatore, secondo una impostazione che appare corretta e opportuna, fornisce chiara indicazione che nel settore pubblico la conservazione debba avvenire con riferimento a standard qualitativi più elevati.

Pertanto, nel caso la conservazione venga affidata in *outsourcing* a conservatori accreditati, il responsabile della conservazione potrà comunque fare conto su una struttura tecnico-organizzativa di supporto, stabile, adeguatamente presidiata e monitorata.

Sarà tuttavia necessario esplicitare, anche contrattualmente, il rapporto tra il responsabile della conservazione e i responsabili nominati presso l'*outsourcer* accreditato, in particolare il rapporto intercorrente con il responsabile del servizio di conservazione, specificando esattamente la ripartizione e il coordinamento delle funzioni.

Ad ogni modo, ai sensi del combinato disposto dell'art. 44, comma 1-*ter*, del CAD, e del comma 2 dell'art. 7 del d.p.c.m. 3 dicembre 2013, "il responsabile della conservazione può chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-*bis*, comma 1, del Codice, distinti dai conservatori o dai conservatori accreditati. Le pubbliche amministrazioni possono chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati, a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44-*bis*, comma 1, del Codice, distinti dai conservatori accreditati".

Il processo di conservazione

In cosa consista esattamente il processo di conservazione digitale a norma, dal punto di vista giuridico e operativo viene delineato dall'art. 9 del d.p.c.m. 3 dicembre 2013, che conviene qui riportare per intero per avere una visione di assieme degli *step* e della attività che lo configurano.

"Art. 9 Processo di conservazione

1. Il processo di conservazione prevede:

a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;

b) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato all'art. 11;

c) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;

d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;

e) l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e la gestione

del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 e secondo le modalità riportate nel manuale della conservazione;

g) la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

h) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;

i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;

j) la produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11, in conformità a quanto previsto dalle regole tecniche in materia di formazione del documento informatico;

k) lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore;

l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

2. Fatto salvo quanto previsto dal decreto legislativo 22 gennaio 2004, n. 42, in ordine alla tutela, da parte del Ministero dei beni e delle attività culturali e del turismo, sugli archivi e sui singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico, i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle stabilite dal presente decreto."

Dalla lettura dell'articolo di legge, si rileva immediatamente l'importanza e la centralità del manuale di conservazione. Su questo tema si ritorna in seguito in maggior dettaglio.

Si osserva anche che l'unica sottoscrizione elettronica (con firma digitale o firma elettronica qualificata) prevista obbligatoriamente dalla normativa e direttamente afferente al processo di conservazione, salvo

ovviamente quanto disposto nel Manuale di conservazione o in altre disposizioni di legge riguardanti altre fasi del ciclo di vita del documento, è quella apposta dal responsabile della conservazione sul PdA (o, meglio sull'indice dello stesso – IPdA); si ritiene che anche tale sottoscrizione, facendo parte del processo di conservazione, possa eventualmente essere delegata.

Il rapporto di versamento è invece un documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore. Può essere generato anche in modo automatico, ma deve essere univocamente identificato dal sistema di conservazione e contenere un riferimento temporale UTC e una o più impronte,[9] calcolate sull'intero contenuto del PdV.

Quindi la funzione di un rapporto di versamento avente esito positivo (il che sostanzialmente significa che il PDV è conforme alle caratteristiche previste dal manuale di conservazione) è giuridicamente estremamente rilevante in quanto attesta il passaggio di consegne dei documenti e dei relativi metadati (o, in casi particolari, anche solo di questi ultimi), e, quindi, delle relative responsabilità, tra il produttore e il responsabile della conservazione. E' in questo senso che deve essere munito di un riferimento temporale (attribuzione informatica di data e ora) di tipo oggettivo e corredato dalle impronte del PdV, in modo che non possano esservi dubbi o contestazioni su quanto, e quando, è stato trasmesso dal produttore e quanto, e quando, è stato ricevuto dal responsabile della conservazione.[10]

La funzione del rapporto di versamento viene ulteriormente chiarita dal d.p.c.m. 13 novembre 2014 agli artt. 7 e 11, entrambi denominati "Trasferimento nel sistema di conservazione", rispettivamente per i documenti informatici *tout-court* e per i documenti amministrativi informatici:

---

[9] La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash* (cfr. d.p.c.m. 3 dicembre 2013, Allegato 1).

[10] Infatti una funzione di *hash* è una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti (cfr. d.p.c.m. 3 dicembre 2013, Allegato 1).

– art. 7, comma 3: "3. Il buon esito dell'operazione di versamento è verificato tramite il rapporto di versamento prodotto dal sistema di conservazione."

– art. 11, comma 1 lettera c): "1. Il responsabile della gestione documentale, ovvero, ove nominato, il coordinatore della gestione documentale: ... c) verifica il buon esito dell'operazione di versamento tramite il rapporto di versamento prodotto dal sistema di conservazione".

Il manuale di conservazione

Il manuale di conservazione è il documento (informatico) fondamentale per la gestione del sistema di conservazione e dei relativi processi.

Il d.p.c.m. 3 dicembre 2013 dedica un apposito articolo a tale documento (Art. 8 – Manuale di conservazione) indicando, al comma 1, le funzioni informative al quale esso deve rispondere.

Al comma 2, vengono elencati in dettaglio gli elementi informativi minimi che lo stesso deve riportare.

"Art. 8 – Manuale di conservazione

1. Il manuale di conservazione illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

2. Il manuale di conservazione è un documento informatico che riporta, almeno:

a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;

b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;

c) la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;

d) la descrizione delle modalità di presa in carico di uno o piu' pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;

e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;

f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;

g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;

h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;

i) la descrizione delle procedure per la produzione di duplicati o copie;

j) i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;

k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;

l) le normative in vigore nei luoghi dove sono conservati i documenti".

Come già visto, la predisposizione del manuale di conservazione e il relativo continuo aggiornamento sono compiti del responsabile della conservazione (art. 7, comma 1, lettera m)).

Si ritiene opportuno anche sottolineare che i conservatori accreditati presso l'AgID devono predisporre (e tenere aggiornato, eventualmente anche in relazione a modifiche richieste dall'AgID stessa) un manuale di conservazione che viene pubblicato e reso liberamente accessibile su web presso la sezione del sito dell'AgID dedicata all'elenco dei conservatori accreditati.

I conservatori accreditati sono obbligati ad attenersi al manuale, da loro predisposto secondo uno schema standard, approvato e pubblicato dall'AgID. Si deve comunque tener presente che i conservatori accreditati possono chiedere che alcune descrizioni di dettaglio, anche ai fini della protezione del proprio know-how, inserite quindi in separata documentazione depositata comunque presso AgID, non vengano rese pubbliche.

In generale, si ritiene consigliabile, per la redazione di manuali di conservazione anche relativi a sistemi interni, attenersi, con tutti gli

opportuni adattamenti, allo "Schema manuale conservazione" (nella versione vigente) pubblicato sul sito dell'AgID.

In tale "Schema" (versione 2, p. 2) viene peraltro chiarito, ovviamente in relazione a un modello organizzativo in cui la conservazione viene affidata in *outsourcing*, in particolare a un conservatore accreditato, che:

"Alcuni elementi indicati all'articolo 8, comma 2, del DPCM del 3 dicembre 2013 riguardano aspetti delle specifiche forniture che non dovranno essere inseriti nel manuale presentato ai fini dell'accreditamento ma dovranno essere sviluppati nell'allegato "Specificità del contratto" del manuale stesso in coerenza e/o facendo riferimento alla documentazione contrattuale prevista dal contratto di servizio stipulato."

Viene inoltre puntualizzato che:

"La predisposizione dell'allegato ed eventuali sue modifiche non sono da considerarsi come modifica del manuale della conservazione e devono essere inviati all'Agenzia per l'Italia digitale solo su espressa richiesta. La verifica dell'allegato è oggetto dell'attività di vigilanza".

Questa ultima indicazione è coerente col fatto che le "specificità del contratto" riguardano la singola fornitura del servizio di conservazione da parte del conservatore accreditato a soggetti terzi; in effetti, ogni singola fornitura potrebbe avere differenti caratteristiche, personalizzazioni, SLA, etc., pur rimanendo coerente con quanto descritto, con applicazione generale nell'erogazione del servizio, nel manuale di conservazione del soggetto accreditato.

Viene inoltre precisato (p. 10) che "il nominativo ed i riferimenti del Responsabile della conservazione devono essere indicati nell'allegato "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione".

Quindi è nell'allegato "Specificità del contratto" che deve essere esplicitato il rapporto funzionale instaurato tra il responsabile della conservazione (nominato presso il produttore o, comunque, il soggetto titolare dei documenti) e il responsabile del servizio di conservazione nominato presso l'*outsourcer* accreditato.

Fondamentalmente, pertanto, il manuale che "governa" la conservazione affidata in *outsourcing* ad un soggetto accreditato sarà formato dal manuale di conservazione del conservatore accreditato, come integrato per quanto riguarda ogni caratteristica (dalle tipologie documentarie, ai formati, alla struttura del PdV, agli SLA, alle politiche di scarto, etc.) della conservazione precipua del singolo produttore, dall'allegato "Specificità del contratto" (a sua volta, se necessario o consigliabile, scindibile in più documenti).

Ricapitolazione: una visione d'assieme

Come risulta evidente dalla pur sintetica esposizione proposta nei paragrafi precedenti, la progettazione, l'implementazione e la gestione di un sistema di conservazione digitale a norma può essere attività impegnativa e complessa, che coinvolge molteplici competenze e strutture organizzative che devono operare in maniera collaborativa e coordinata.

Si tratta quindi anche di attività che richiede disponibilità di risorse umane e finanziarie adeguate.

Ovviamente, la complessità e l'onerosità del sistema di conservazione sono direttamente correlate alla numerosità e alle tipologie dei documenti da conservare e alle caratteristiche delle strutture organizzative che devono usufruire della conservazione, nonché all'estensione della *community* di utenti che deve potervi accedere. Un altro elemento di valutazione importante è anche quello che riguarda la necessità di caratteristiche prestazionali elevate strumentali al supporto di flussi e accessi massivi, numerosi e ad alta frequenza.

Sistemi di conservazione che devono gestire quantità limitate di documenti rientranti in poche tipologie standard e, che soprattutto, non debbano essere aperti nell'accesso a *community* estese e in continuo mutamento, possono comunque essere gestiti *in-house* anche da soggetti non particolarmente strutturati, in particolare grazie all'ausilio di soluzioni software, facilmente reperibili sul mercato, in grado di automatizzare la creazione di PdV, PdA e PdD e di gestire le funzioni di firma elettronica e di back-up.

Non è infatti infrequente che i medesimi operatori di settore siano in grado di fornire supporto sia per soluzioni *in-house* sia per soluzioni in *outsourcing*, come pure non è raro che soluzioni di gestione documentale interne vengano integrate con sistemi di conservazione esterni.

Bisogna quindi considerare che la "complicazione" sottesa a un sistema di conservazione, peraltro per molti aspetti decisamente inferiore a quella ai altri sistemi informativi di uso comune, viene risolta a livello progettuale, risultando in una implementazione di servizi e di soluzioni software *user-friendly* il cui utilizzo comporta un impegno operativo veramente limitato.

Il tempo necessario per l'archiviazione, lo stoccaggio, la ricerca, di un documento cartaceo può risultare di gran lunga superiore a quello di un documento informatico, e già per volumi documentali non particolarmente rilevanti, miglioramenti significativi in termini di efficienza e di efficacia sono quasi immediatamente percepibili.

Se poi le valutazioni includono le infrastrutture necessarie alla gestione cartacea (spazi fisici sicuri, *device* di stampa e riproduzione, movimentazione, fruibilità, etc.), la conservazione digitale vince di gran lunga il confronto sia sul piano organizzativo che su quello economico.

Nell'introduzione dell'argomento si è già messo in evidenza come la conservazione sia solo una fase, anche se tipicamente la più lunga, del ciclo di vita del documento. La sua funzione è al contempo neutrale ed essenziale:

– neutrale, sia nel senso che non entra nel merito del perché si sia formato un documento, sia nel significato che anche una conservazione eseguita a regola d'arte non può correggere eventuali vizi di formazione dello stesso;

– essenziale, in quanto finalizzata alla preservazione, anche nel lungo periodo, del documento, sia nel suo contenuto e nella sua intelligibilità di carattere informativo, sia nella sua validità giuridica.

Inoltre la conservazione non deve essere considerata una fase statica; aldilà delle più ovvie considerazioni riguardanti la preservazione dell'utilizzabilità dei documenti gestiti mediante strumenti e formati in continua evoluzione quali sono quelli dell'ICT, vi sono da gestire dinamicamente e in maniera sicura gli accessi, la produzione di PdD o di duplicati/estratti/copie di documenti (anche in aggregazione, quali fascicoli, dossier, cartelle, etc.), eventuali ri-classificazioni documentarie, etc., il tutto in un contesto normativo necessariamente fluido, in quanto anch'esso correlato all'evoluzione tecnologica.

In sintesi, il sistema di conservazione è sua volta anche un produttore di documenti, i quali devono rispondere a precise esigenze informative e giuridiche.

Quindi, la conservazione è una fase del ciclo di vita del documento concettualmente e giuridicamente isolabile dalle altre, ma la validità informativa e giuridica di un documento dipende dalla corretta esecuzione di tutto quanto ne supporta il ciclo di vita.

Anche il legislatore ha rimarcato l'assoluta necessità che i responsabili - come ovviamente le relative strutture organizzative - della conservazione, del trattamento dei dati personali, della sicurezza, dei sistemi informativi e della gestione documentale "operino d'intesa" proprio perché la preservazione di lungo periodo di un contenuto informativo, con rilevanza anche giuridica, è attività intrinsecamente interdisciplinare.

I documenti informatici devono essere correttamente formati, conformemente alla normativa; sin dalla loro formazione agli stessi

devono essere associati almeno i metadati minimi obbligatori per legge (cfr. d.p.c.m. 13 novembre 2014) e quelli previsti dalla normativa speciale di contesto (ad esempio nelle pubbliche amministrazioni, dal manuale di gestione documentale). Da una adeguata associazione dei metadati discende immediatamente la fruibilità dei contenuti informativi, quindi, ovviamente, sia la gestione dell'archivio corrente, sia la gestione dell'archivio di deposito richiedono da subito l'individuazione di ulteriori metadati, rispetto a quelli obbligatori, funzionali alla gestione delle informazioni, individuati seguendo, tra l'altro, i criteri della migliore dottrina archivistica.

I contenuti informativi e i relativi metadati devono essere correttamente "accorpati" dal produttore – nelle pubbliche amministrazioni nell'ambito di azione del responsabile della gestione documentale -, ai fini del trasferimento in conservazione, in pacchetti di versamento (PdV) compatibili con le specifiche esplicitate nel manuale di conservazione e, nel caso dell'*outsourcing*, nelle eventuali "specificità del contratto" concordate, ai fini di una corretta formazione dei pacchetti di archiviazione (PdA), la quale invece avviene nella sfera di competenza del responsabile della conservazione. Con la presa in carico, attestata da un rapporto di versamento avente esito positivo, il responsabile della conservazione si impegna a formare PdA conformi alla legge e a quanto concordato con il produttore e a rendere disponibili le informazioni, mediante pacchetti di distribuzione (PdD) alle *community* di utenti, opportunamente profilate, anche nei diritti di accesso. Tutto questo, oltre che per obbligo di legge, per ovvie necessità tecnico giuridiche, deve avvenire con il coinvolgimento dei responsabili dei sistemi informativi, della sicurezza e del trattamento dei dati personali.

A questo punto risulterà chiaro, e condivisibile, il perché il d.p.c.m. 3 dicembre 2013 (conservazione), il d.p.c.m. 3 dicembre 2013 (protocollo) e il d.p.c.m. 13 novembre 2014 ("formazione") condividano gli stessi allegati tecnici.

Approfondimento I: il responsabile della conservazione

Si è visto come, sia nel CAD che nel d.p.c.m. 3 dicembre 2013, il responsabile della conservazione sia figura centrale nella gestione del sistema di conservazione. Deve anche risultare chiaro che tale figura non coincide con il responsabile del servizio di conservazione nominato obbligatoriamente dai conservatori accreditati e il cui curriculum viene

valutato nella sua adeguatezza a rivestire tale ruolo dalle funzioni preposte dell'AgID.

Peraltro, laddove l'*outsourcer* non sia un conservatore accreditato, caratteristica obbligatoria solo per l'affidamento della conservazione da parte delle pubbliche amministrazioni, il ruolo del responsabile del servizio di conservazione può anche non sussistere o essere denominato e configurato in maniera diversa da quella prevista per i conservatori accreditati.

Rispetto alle pubbliche amministrazione è alquanto pacifica l'interpretazione secondo la quale, in base all'art. 7, comma 3, del d.p.c.m. 3 dicembre 2013, il ruolo debba obbligatoriamente[11] essere svolto,

[11] Le residue perplessità interpretative circa l'obbligatorietà dello svolgimento del ruolo da parte di in soggetto interno (dirigente o funzionario) alla pubblica amministrazione derivano anche dal fatto che il termine "ruolo" viene utilizzato in senso generico, vale a dire con significato diverso a quello che tecnicamente comunemente assume nel diritto amministrativo e nel diritto pubblico. D'altra parte, come già più volte visto, "la conservazione può essere affidata a un soggetto esterno" (anche privato, ancorché accreditato), il che conduce ad una difficile inquadramento della conservazione stessa come funzione (amministrativa) o come servizio (anche pubblico, nel senso che è parzialmente svolto nel diretto interesse di soggetti privati, peraltro già posto sotto il controllo dell'AgID nell'ambito dei poteri di vigilanza sui conservatori accreditati), a sua volta distinzione sempre meno netta e sempre più fluida sia nel diritto dell'Unione, che nel diritto amministrativo nazionale, pur, forse, rimanendo sempre intravvedibile un rapporto di strumentalità dell'uno rispetto all'altra. Le Linee guida AgID fanno riferimento al concetto di servizio (ad esempio, p. 62: "Le pubbliche amministrazioni che vogliano esternalizzare il servizio di conservazione, sono tenute per legge ad affidarlo ad una società, sia essa pubblica o privata, accreditata presso AgID, di cui all'articolo 44-*bis* del CAD."). Altrove (p. 93), nel caso l'affidamento avvenga nei confronti di un soggetto pubblico, riemerge in concetto di funzione: "Nel caso della conservazione l'interesse comune tra produttore e soggetto conservatore si può identificare nel reciproco interesse alla corretta conservazione del patrimonio documentale pubblico: obbligo di legge per l'ente produttore e funzione specifica di un conservatore pubblico". In conclusione, la lettura alternativa della norma in questione potrebbe essere la stessa serve a specificare che il responsabile deve essere un dirigente o un funzionario quando il servizio viene svolto all'interno, ma non quando viene esternalizzato, peraltro a società lucrative e comunque sotto il controllo dell'AgID.

La gestione documentale, già nel d.p.r. 445/2000 (vedi art. 61), è qualificata come servizio (con connotazione decisamente più interna che esterna), ed allo stesso è preposto senza dubbio un dirigente o un funzionario interno, ma il servizio non è esternalizzabile.

mediante designazione formale, da un dirigente o da un funzionario, eventualmente già nominato anche responsabile della gestione documentale.

Più dibattuta è invece la questione della "collocazione" del responsabile della conservazione rispetto ai soggetti giuridico-economici che non rientrino nel novero delle pubbliche amministrazioni.

Il problema è risalente e si deve anche ricordare che in vigenza della Deliberazione Cnipa n. 11/2004 la prassi di gran lunga più utilizzata, nel caso dell'affidamento in *outsourcing* della conservazione, è stata comunque quella di delegare, anche seguendo diverse modalità giuridico-contrattuali per farlo, tale ruolo presso l'*outsourcer*, e questo anche nel caso delle pubbliche amministrazioni.

La netta prevalenza della soluzione di "esternalizzare" il ruolo è stata basata su come il testo dell'art. 5 (Responsabile della conservazione), comma 2, della Deliberazione Cnipa n. 11/2004 è configurato:[12] il fatto che tutte le attività del responsabile potessero essere delegate ad altri ha lasciato spazio al pensiero che, potendosi "svuotare" il ruolo, di conseguenza anche quest'ultimo potesse essere delegato in toto.

In conclusione, l'elemento interpretativo decisivo ha forse più natura teleologico-sistematica, che non letterale: i commi 1-*bis* e 1-*ter*, dell'art. 44 del CAD (entrato in vigore il 25/01/2011), hanno fino all'11 aprile 2014 convissuto esclusivamente con la Deliberazione Cnipa n. 11/2004, che nulla specificava in proposito, e che, semmai, si è prestata a interpretazioni opposte (vedi anche di seguito nel testo). All'inserimento del comma 3 (e anche del comma 4), nell'art. 7 del d.p.c.m. 3 dicembre 2013 può quindi essere attribuito un significato chiarificatore dell'intenzione del legislatore di mantenere un controllo interno all'ente produttore anche in caso di affidamento all'esterno. Certamente un aspetto così essenziale avrebbe dovuto essere regolato in maniera amministrativamente più tecnica e all'interno della norma primaria (il CAD) e non della norma derivata (il d.p.c.m. 3 dicembre 2013).

[12] Si usa il presente, perché, in base all'art. 14 del d.p.c.m. 3 dicembre 2013, rispetto a soggetti che stanno utilizzando sistemi di conservazione non ancora aggiornati alle nuove regole tecniche, la Deliberazione è ancora applicabile.

Il testo del comma 2 richiamato nel testo è il seguente:

"2. Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate".

Tale interpretazione veniva poi corroborata in base al disposto del comma 3 dello stesso articolo,[13] sottolineando le affermazioni secondo le quali il procedimento di conservazione potesse essere affidato totalmente in *outsourcing* e, soprattutto, che i soggetti affidatari del servizio di conservazione fossero gravati da un autonomo obbligo di rispetto della deliberazione stessa.

Su questa base interpretativa entravano poi in gioco altre considerazioni di tipo decisamente pratico: dalla difficoltà di reperire, o formare e remunerare, un soggetto con le competenze necessarie per rivestire un ruolo essenzialmente innovativo e interdisciplinare (essendo molto più semplice risolvere il problema reperendolo presso un *outsourcer* specializzato), alla maggior appetibilità commerciale di una soluzione di *outsourcing* "chiavi in mano". Non da ultimo entravano in considerazione valutazioni di tipo operativo e contrattualistico, apparendo più congruo che il responsabile della conservazione, nel caso dell'*outsourcing*, potesse essere un soggetto, sì responsabilizzato verso il committente, ma che avesse un controllo diretto sul sistema di conservazione gestito presso una entità economico-giuridica terza.

Con l'entrata in vigore del d.p.c.m. 3 dicembre 2013, come si è già ricordato, rimane ancora dibattuta, nel settore privato, in assenza di una esplicita espressione normativa quale il già ricordato comma 3 dell'art. 7 del d.p.c.m. 3 dicembre 2013, la questione se la nomina del responsabile della conservazione debba essere necessariamente effettuata, contrariamente a quanto generalmente avveniva in passato nel caso dell'*outsourcing*, nella sfera giuridica del soggetto che deve/vuole conservare i documenti in digitale o, se tale nomina possa anche non essere effettuata del tutto.[14]

---

[13] "3. Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione".

[14] Tale seconda ipotesi aveva trovato un suo esplicito riferimento in quanto asserito al punto 7.4. della Circolare 36E/2006:

"Il responsabile della conservazione di norma si identifica con il contribuente, salva la facoltà di quest'ultimo di designare un terzo; nel caso di contribuenti diversi dalle persone fisiche, spetta agli stessi il potere di nominare il responsabile della conservazione che potrà essere sia un soggetto legato da un rapporto qualificato (un socio o un amministratore) sia un terzo esterno alla società, all'associazione o all'ente".

Per prima cosa si osserva che anche la Circolare citata ammetteva che il responsabile potesse essere un soggetto esterno a chi era, in base alla normativa tributaria, obbligato alla conservazione dei documenti (il contribuente), in questo caso in forma digitale.

Invece l'affermazione che "Il responsabile della conservazione di norma si identifica con il contribuente …" appare discutibile e sembra confondere una responsabilità generica e generale del contribuente, il quale comunque è il soggetto che ha l'obbligo di legge di conservare i documenti (in questo caso a rilevanza tributaria), con una responsabilità specifica e speciale, come configurata (anche allora) dalle relative regole tecniche, vale dire quella del responsabile della conservazione.

Peraltro, ovviamente, l'interpretazione dell'Agenzia delle Entrate poteva riguardare solo gli aspetti tributari della questione.

Ad ogni modo, le modifiche apportate al CAD, successivamente all'emanazione della Circolare 36E/2006, portano ad escludere che in assenza di esplicita nomina, contribuente (oppure, più in generale, il soggetto obbligato o interessato alla conservazione dei documenti) e responsabile della conservazione coincidano, mentre resta condivisibile che, in ogni caso, vale a dire sia in caso di nomina o meno del responsabile, il contribuente risponda della conservazione.

Nel CAD di oggi è auto-evidente che i processi e il sistema di conservazione sono incardinati attorno alla figura del responsabile della conservazione, e questo a partire dal disposto del comma 1-*bis* dell'art. 44: "Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa … nella definizione e gestione delle attività di rispettiva competenza.".

E' palese che se il legislatore avesse voluto attribuire la gestione del sistema di conservazione al soggetto giuridico obbligato o interessato ad eseguirla, non avrebbe evocato una specifica figura di responsabile affiancandola ad altre di cui non può discutersi la necessaria esistenza con le quali coordinarsi.

Appare quindi del tutto sconsigliabile non procedere alla nomina formale del responsabile della conservazione, anche sulla base delle seguenti ulteriori considerazioni:

– ferma restando la responsabilità del soggetto giuridico obbligato alla conservazione dei documenti, la colpa potrebbe essere aggravata dal fatto di non essersi avvalso di un responsabile "tecnico", sul quale peraltro eventualmente rivalersi;

– insomma, potrebbe essere contestata al soggetto giuridico, o a chi lo rappresenta, una, per così dire, si passi l'espressione, "culpa in non

eligendo", nel senso di non avere individuato un soggetto tecnicamente adeguato alla gestione della conservazione digitale a norma;

– se si volesse seguire una traccia interpretativa ancora più estrema, mancando il responsabile della conservazione, vista la sua centralità giuridico-operativa rispetto alla stessa, potrebbe anche contestarsi la congruità giuridica della conservazione stessa e, di conseguenza, la piena validità legale dei documenti conservati.

Chiarito e motivato il perché, a parere di chi scrive, sia assolutamente da evitarsi il non nominare formalmente il responsabile della conservazione, rimane da affrontare la questione più dibattuta, vale a dire se sia possibile farlo presso l'*outsourcer* o, comunque, utilizzando soggetti "esterni".

Innanzitutto si osserva che, pur non esistendo per il settore privato una disposizione simile a quella già vista per le pubbliche amministrazioni, il disposto del comma 6 dell'art. 6 apporta alcune lievi, ma significative variazioni, a quanto previsto dal comma 2 dell'art. 5 della Deliberazione Cnipa n. 11/2004.

L'aggiunta dell'inciso "sotto la propria responsabilità" fa innanzitutto escludere che la delega totale del processo di conservazione "svuoti" di contenuto il ruolo, in quanto, appunto, resta ferma la responsabilità del responsabile della conservazione, il quale quindi deve necessariamente esistere ed essere specificamente individuato.

Anche il successivo comma 7, in tema di affidamento a soggetti esterni della conservazione, rafforza tale interpretazione, laddove si afferma che il contratto o la convenzione di servizio devono prevedere l'obbligo del rispetto del manuale della conservazione predisposto dal responsabile della stessa.

Tornando al comma 6, è interessante osservare che mentre la Deliberazione Cnipa n. 11/2004, all'art. 5, comma 2, parlava di una delega "ad una o più persone", il d.p.c.m. 3 dicembre 2013 si esprime in termini di delega "a uno o più soggetti", questo portando a pensare che la delega possa essere attuata anche verso soggetti diversi dalle persone fisiche.

Sulla questione principale, l'AgID ha espresso la propria posizione in una FAQ pubblicata sul proprio sito,[15] dove viene affermato che il ruolo di responsabile della conservazione può essere ricoperto esclusivamente

---

[15] Cfr. http://www.agid.gov.it/faq/ruoli-coinvolti-processo-conservazione, "Ruoli coinvolti nel processo di conservazione", "Ultimo aggiornamento 22 Maggio 2015":

da una persona fisica alle dipendenze del soggetto produttore dei documenti essendo questo valido anche per i soggetti privati.

Aldilà del "peso" giuridico che si voglia attribuire ad una FAQ, non è chiaro quale sia, nel settore privato, la disposizione normativa che stabilisca che il responsabile della conservazione debba essere un "dipendente" del soggetto produttore dei documenti. Forse può intendersi l'espressione "alle dipendenze" in senso più lato, attribuendole il significato che la nomina (o il mandato) debba comunque provenire dal produttore ed essere collocata nella propria sfera giuridico-organizzativa.

Certamente la FAQ esclude che il responsabile della conservazione possa essere "alle dipendenze" dell'*outsourcer*.

Altra affermazione importante è che il responsabile della conservazione è una persona fisica, aspetto questo che appare congruente con l'assetto normativo attualmente vigente.

Sempre da parte dell'AgID il tema ha subito una più estesa e profonda rielaborazione nelle Linee guida AgID sulla conservazione, di recente redazione. Anche qui (p. 67) viene ribadito che "Il Responsabile della conservazione è la persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato."

In buona sostanza, l'AgID esclude che il responsabile della conservazione possa gravitare nella sfera giuridica dell'*outsourcer* è questo è motivato nella misura in cui verrebbero meno, dal punto di vista sostanziale, funzioni essenziali quali quelle del controllo, della vigilanza sull'operato del soggetto esterno, nonché quella della continuità nel ruolo presso il produttore.

"In caso di affidamento del servizio di conservazione in outsourcing a un soggetto pubblico o privato il ruolo di Responsabile della conservazione può essere svolto da una persona fisica alle dipendenze del soggetto affidatario del servizio?"

"No, il ruolo di Responsabile della conservazione può essere ricoperto esclusivamente da una persona fisica alle dipendenze del soggetto produttore dei documenti da conservare, che affida le attività di conservazione al Responsabile del servizio di conservazione.

Coerentemente con quanto indicato in relazione ai soggetti a cui si applicano le regole tecniche di conservazione, tale vincolo vale per tutti i soggetti, anche i privati."

L'AgID inoltre ribadisce la necessità di designare formalmente il responsabile della conservazione (*ibidem*, p. 64): "A prescindere dal modello adottato [*in-house* o in *outsourcing*, N.d.R], rimane l'obbligo di nominare all'interno dell'organizzazione la figura del responsabile della conservazione …".

Come si è visto, l'AgID, nelle Linee guida, ha abbandonato il concetto di un responsabile della conservazione "alle dipendenze", sostituendolo con i concetti di "persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti" o di "nomina all'interno dell'organizzazione".

Si tratta di concetti comunque giuridicamente non ben definiti e che non risolvono il problema di quale debba essere la collocazione del responsabile della conservazione rispetto al soggetto obbligato o interessato alla conservazione digitale a norma dei documenti.

In particolare, si tratta di concetti di difficile applicazione in contesti aziendali, di lavoro autonomo o artigianali di dimensioni minime, i quali potrebbero anche non avere alcun organico o organizzazione interna, o comunque non disporre di risorse sufficientemente qualificate per rivestire il ruolo di responsabile della conservazione.

Da tali concetti alquanto indefiniti, si possono tuttavia astrarre principi condivisibili, vale a dire quello della necessità della continuità della sussistenza del ruolo ("inserimento stabile nell'organico") e quello della certezza che il responsabile della conservazione operi nell'esclusivo interesse del soggetto produttore, a questi peraltro rispondendo ("nomina all'interno dell'organizzazione").

Non si intravvede tuttavia una chiara motivazione, giuridica o organizzativa, del perché nel ruolo non possa essere designato un professionista munito delle necessarie competenze e capacità, il quale comunque potrebbe muoversi, all'interno del mandato ricevuto e secondo le condizioni economiche concordate, peraltro anche nei limiti dei codici deontologici eventualmente applicabili, "con piena responsabilità ed autonomia", come richiesto dal comma 5 dell'art. 6 del d.p.c.m. 3 dicembre 2013.

D'altra parte, la conservazione di documentazione di titolarità altrui e nell'altrui interesse, anche in ottemperanza ad un obbligo di legge, già da tempo, direi immemorabile, può avvenire presso professionisti esterni, quali notai, commercialisti, consulenti del lavoro, avvocati, archivisti, etc., i quali la organizzano in autonomia e seguendo le disposizioni di legge, comunque rispondendone, in base al mandato professionale, al titolare dei documenti.

Peraltro, in generale, la normativa non esclude che si possano utilizzare più sistemi di conservazione digitale, situazione peraltro non infrequente laddove gli archivi siano decentrati, ovvero si debbano conservare documenti di tipologie estremamente differenziate. Vuoi la delocalizzazione, vuoi la necessità di una particolare specializzazione rispetto ai documenti conservati potrebbe consigliare la nomina di più delegati od anche di più responsabili della conservazione,[16] nel secondo caso in base al possesso di determinate competenze. E' infatti chiaro che l'interlocuzione con i soggetti e le Autorità che devono/possono accedere agli archivi potrà essere meglio gestita da figure che meglio conoscono il contesto normativo rispetto al quale i documenti devono essere prodotti. Conservati ed esibiti.

Comunque, a livello sostanziale, se il vero scopo di nominare un responsabile esterno all'*outsourcer* è, in ultima analisi, quello di poter contare su una funzione di controllo qualificato dell'operato dello stesso,

---

[16] Non è immediato se sia possibile, nel silenzio della normativa, nominare, nel settore privato, più responsabili della conservazione.

Per quanto riguarda le pubbliche amministrazioni, la normativa non riprende quanto disposto dal d.p.c.m. 3 dicembre 2013 (protocollo) dove, all'art. 3, lettera b), è previsto che il responsabile della gestione documentale è nominato per ciascuna area organizzativa omogenea, e, alla lettera c) è prevista l'eventuale nomina di un coordinatore della gestione documentale, in presenza di più aree organizzative omogenee. Il comma 4 dell'art. 7 del d.p.c.m. 3 dicembre 2013 (conservazione) prevede che il ruolo possa essere assunto dal coordinatore della gestione documentale, se nominato. Poiché, appunto, la nomina del coordinatore è eventuale, deve ipotizzarsi la compresenza di più responsabili della conservazione afferenti a ciascuna area organizzativa omogenea.

Quindi, anche nel settore privato, non si può escludere, in base alla lettera della norma, la possibilità di nominare più responsabili della conservazione, i confini della cui competenza dovranno comunque essere dettagliatamente determinati. Peraltro il modello sarebbe simile a quanto avviene per il responsabile del trattamento (cfr. art. 29, comma 3, del D.Lgs. 196/2003: "Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.").

In ogni caso, anche nel settore privato, devono essere assunte misure per garantire la continuità nel ruolo. Il problema non è di semplicissima soluzione nella pratica; potrà essere adottato un modello simile a quello che nel settore pubblico viene adottato per il responsabile della gestione documentale o per il coordinatore della gestione documentale, per i quali devono essere nominati anche i rispettivi vicari "per casi di vacanza, assenza o impedimento" (art. 3, comma 1, lettere b) e c) del d.p.c.m. 3 dicembre 2013 – protocollo).

Si ritiene che la nomina del vicario, che dovrebbe anch'esso essere una persona fisica, debba provenire dallo stesso organismo competente a nominare il responsabile della conservazione.

è evidente che tale funzione potrà essere meglio svolta da un professionista competente, che non da un operatore economico, magari individuale, che di tutt'altro si occupa e si deve occupare.

Ad ogni modo, è certo che gli strumenti dell'affidamento e della delega, unitamente al fatto, pacifico, che il responsabile della conservazione possa comunque avvalersi di assistenza e consulenza specializzata, fanno sì che il ruolo possa fondamentalmente assumere le connotazioni di una attività di coordinamento, ragionato e interdisciplinare, e di controllo. Altrimenti detto, il ruolo può anche non assumere i connotati di un'attività operativa intensa e impegnativa.

Certamente l'idea interpretativa che l'*outsourcer* non possa più offrire, come avveniva in passato, un servizio "chiavi in mano" comprensivo dell'assunzione del ruolo di responsabile della conservazione, può avere un impatto sulle regole del mercato di settore, in quanto, comunque, l'attribuzione di una (nuova) responsabilità potrà disincentivare l'approccio spontaneo alla conservazione digitale o, comunque, aumentarne i costi, il che dovrebbe stimolare perlomeno qualche riflessione.

Approfondimento II: aspetti contrattualistici

Le ultime brevi riflessioni sui temi della delega e dell'affidamento portano inevitabilmente a ragionare sui temi contrattualistici connessi alla conservazione digitale. Tralasciando di analizzare la contrattualistica del settore pubblico, la cui specialità richiederebbe una trattazione che trascende gli spazi e gli scopi del presente articolo, può essere opportuno delineare qualche punto fermo riguardante il settore privato, in particolare quando la conservazione viene affidata in *outsourcing*.

– Una volta che si è stabilito che si vuole o si deve adottare la conservazione digitale a norma, il primo passaggio giuridico e logico-progettuale dovrebbe consistere nella nomina formale, da parte dell'organismo interno competente, del responsabile della conservazione.

– Infatti non bisogna dimenticare che il responsabile della conservazione ha innanzitutto una funzione progettuale (art. 7, comma 1, lettera a) del d.p.c.m. 3 dicembre 2013) di definizione dei requisiti del sistema, rispetto alle tipologie documentarie da conservare, in maniera conforme alla normativa vigente.

– Se i sceglie di designare un soggetto già inquadrato o da inquadrare stabilmente nella struttura organizzativa del produttore è opportuno che

venga scelta una persona, non solo competente, ma che abbia anche potere decisionale, di spesa, e risorse a disposizione, questo conformemente a un principio giuridico generalissimo che vorrebbe che una responsabilità sia correlata alla disponibilità degli strumenti per farsene carico.

– Sarebbe anche opportuno che il responsabile, nell'ambito delle attività di cui si deve occupare, abbia il potere di sottoscrizione di contratti, o, perlomeno, una funzione di controllo e approvazione degli stessi, anche perché, come già visto, ad esempio i contratti di outsourcing della conservazione devono obbligatoriamente prevedere il rispetto del manuale di conservazione.[17]

– Devono essere dettagliati i poteri di delega, stabiliti in senso generale dal comma 6 dell'art. 6 del d.p.c.m. 3 dicembre 2013, e il processo formale con cui le deleghe vengono rilasciate sia a soggetti dell'organizzazione di appartenenza, che a soggetti esterni alla stessa.

– Devono essere stabiliti i poteri di rappresentanza, ad esempio verso l'*outsourcer* e verso chiunque abbia un interesse o un dovere di avere accesso ai documenti (*stakeholder*, *auditing*, autorità preposte a accessi, ispezioni, verifiche, etc.).

– In sintesi, doveri e poteri attribuiti in senso generale al ruolo dalla normativa devono necessariamente essere dettagliati nel mansionario dell'organizzazione, compresi quelli degli eventuali delegati interni.

– In buona sostanza, per tutte le precedenti motivazioni, può risultare opportuno designare una figura di tipo apicale.

– Qualora si ritenesse valida l'idea interpretativa di poter nominare una figura esterna, di tipo professionale, la nomina dovrebbe comunque essere opportunamente circostanziata, determinando esattamente i confini del mandato professionale, in particolare per quanto riguarda corrispettivi, doveri e poteri attribuiti, facoltà di delega, poteri di rappresentanza (ad esempio verso l'*outsourcer* e verso chiunque abbia un

---

[17] Il già citato art. 44 comma 1-*ter* del CAD prevede, con espressione alquanto a-tecnica ("chiedere"), che "Il responsabile della conservazione può chiedere la conservazione dei documenti informatici … ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche". Il principio generale viene poi declinato nel d.p.c.m. 3 dicembre 2013, art. 6, comma 7, nel concetto di affidamento, ma espresso in forma impersonale: "7. La conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all'art. 5, …".

Deve quindi essere assolutamente chiarito chi all'interno del produttore debba/possa intervenire nella sottoscrizione dei contratti di *outsourcing* correlati alla conservazione.

interesse o un potere/dovere di avere accesso ai documenti) durata, rinnovi, cause di cessazione naturali, straordinarie o patologiche (vizi del sinallagma funzionale), penali, foro competente, etc.: in sintesi, dovrebbe essere configurato un vero e proprio contratto, opportunamente corredato da tutto quanto necessita per declinare, integrare e dettagliare quanto disposto dalla normativa in termini generali.

– Non ci si dilunga sui criteri di selezione dell'*outsourcer*. I parametri di riferimento sono abbastanza intuitivi: accreditamento, esperienza e fatturato nel settore, referenze, solidità economico-finanziaria, dimensioni e qualità della struttura organizzativa, pregressa e prevedibile persistenza sul mercato o, in generale, prevedibile durata del soggetto giuridico, non sussistenza di contenziosi, coperture assicurative (obbligatorie per i conservatori accreditati), buon bilanciamento tra condizioni economiche offerte e requisiti qualitativi garantiti.

– Può in ogni caso essere opportuna un'attività preventiva e ripetuta nel tempo di *audit*, quest'ultima opportunamente regolata contrattualmente. Si ritiene che il riferimento principale per tale attività possa essere lo standard ISO 16363-2012 - *Audit and certification of trustworthy digital repositories.*[18]

– Per quanto riguarda i contratti di outsourcing, gli schemi contrattuali correntemente in uso, nel silenzio della norma, si atteggiano sostanzialmente come contratti di appalto, contratti misti, contratti complessi, contratti atipici, contratti innominati[19] o anche come contratti collegati.[20]

---

[18] Cfr. anche http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510: *Abstract "ISO 16363:2012 defines a recommended practice for assessing the trustworthiness of digital repositories. It is applicable to the entire range of digital repositories. ISO 16363:2012 can be used as a basis for certification."*

[19] Nel testo non si vuole entrare nel merito delle sottili disquisizioni dottrinali che differenziano o assimilano, totalmente o parzialmente, contratti misti, complessi, atipici e innominati. Lo scopo è di attirare l'attenzione sul fatto che quando si esce da uno schema tipico, il quale peraltro ovviamente non potrebbe essere individuato solo in base al *nomen iuris* attribuito, bisogna prestare attenzione alla corrispondenza tra la fattispecie e lo schema contrattuale adottato, eventualmente anche alla luce dell'applicabilità delle teorie interpretative dell'assorbimento e della combinazione.

[20] Una certa complicazione contrattuale può derivare dal fatto che assieme alla conservazione vengono erogati altri servizi collegati o accessori (firma digitale, marcatura temporale, attivazioni, interfacce web, personalizzazioni, fatturazione elettronica verso la P.A., P.E.C., digitalizzazione del pregresso cartaceo, assistenza trasversale, etc.), il tutto dovuto in parte anche alla necessità degli operatori di

– Si deve verificare l'assoggettabilità del servizio al disposto del D.Lgs. 70/2003, verifica quasi sempre positiva, e prestare attenzione al fatto che alcune norme dello stesso sono derogabili solo nei confronti di operatori economici professionali, ma non dei consumatori.

– Del pari, nel caso il produttore sia un consumatore, il contratto dovrà essere adeguato a quanto previsto per il caso dal codice civile e dal Codice del Consumo.

– Unica regola esplicitamente contrattuale posta dal d.p.c.m. 3 dicembre 2013 è il già più volte ricordato comma 7 dell'art. 6 che impone che il contratto preveda l'obbligo di rispetto del manuale di conservazione predisposto dal responsabile della stessa.

– Tale regola pone il manuale al centro dell'assetto contrattuale, in particolare per tutto ciò che riguarda l'oggetto della controprestazione del fornitore, le modalità di erogazione ed utilizzo del servizio, la organizzazione ad esso strumentale, la ripartizione delle attività operative e delle relative responsabilità, i livelli di servizio, anche rispetto alle diverse tipologie documentarie, le misure di sicurezza,[21] la tutela della riservatezza dei dati e delle informazioni etc.. Si ricorda inoltre che ai sensi del comma 8 dell'art. 6 del d.p.c.m. 3 dicembre 2013, il "soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali." Per quanto l'assunzione avvenga *ope legis*, tuttavia può essere opportuno, anche per ragioni pratiche di "portabilità" dell'attribuzione/assunzione del ruolo, formalizzare comunque un documento specifico,[22] corredato dall'informativa ai sensi dell'art. 13 del D.Lgs. n. 196/2003 e dal relativo consenso.

---

configurare offerte commerciali flessibili. Spesso, anche il solo servizio di conservazione va a includere fasi del processo di gestione documentale. Tuttavia i servizi offerti congiuntamente spesso riguardano processi troppo differenziati per poter convivere coordinatamente in un unico contratto, anche perché a volte i singoli servizi sono, nei fatti, gestiti da operatori diversi, secondo concatenazioni più o meno intelligibili, in particolare dal punto di vista della ripartizione delle responsabilità.

A parere di chi scrive può allora essere consigliabile utilizzare lo schema del contratto quadro, nel contesto del quale inserire in maniera coordinata, ma anche indipendente, singoli moduli di servizio compiutamente descritti e regolati nelle loro peculiarità.

[21] Al tema della sicurezza dei sistemi di conservazione viene dedicato un apposito articolo del presente Quaderno.

[22] Anche in relazione al fatto che il comma 2 del D.Lgs. 196/2003 prevede che "I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare".

– Si è già ricordato che i conservatori accreditati devono depositare presso l'AgID, il proprio manuale di conservazione, per la necessaria approvazione e pubblicazione. Altra documentazione tecnica integrativa può essere depositata, tuttavia con riserva di non pubblicazione, sostanzialmente ai fini della tutela del *know-how* del conservatore. I conservatori accreditati devono attenersi a tale manuale, per cui, sostanzialmente il manuale di conservazione del soggetto produttore sarà, per così dire, composto dal manuale del conservatore e dall'allegato che l'AgID ha definito "specificità del contratto", vale a dire relativo a tutti gli elementi di dettaglio operativo e alle personalizzazioni che devono essere configurati per erogare il servizio in funzione delle esigenze dello specifico produttore, come concordate col responsabile della conservazione, sulla base dei requisiti del sistema di conservazione da questo delineati. Tale allegato, nei fatti, sarà composto da una serie di documenti tecnico-giuridici di dettaglio. Di particolare importanza, nel modello OAIS, è la definizione delle community di utenti e i relativi diritti di accesso al sistema.[23]

– Quindi, in sostanza, l'obbligo di rispetto del manuale previsto dall'art. 6, comma 7, del d.p.c.m. 3 dicembre 2013, si declina in un obbligo di rispetto del manuale del conservatore accreditato e della documentazione componente le "specificità del contratto" concordate.

– A livello operativo, si ritiene consigliabile accorpare, o, perlomeno, collegare in maniera sistematica, tale documentazione, per configurare il manuale di conservazione approvato dal responsabile della conservazione, il quale, peraltro, ai sensi della lettera m) dell'art. 7, comma 1, del d.p.c.m. 3 dicembre 2013 ne deve curare il *versioning* (vale dire, ai termini di legge, "l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti".) Ovviamente, tale attività potrà, anzi, dovrà essere svolta in collaborazione con l'*outsourcer*, con il quale dovranno anche essere verificate le conseguenze sull'impianto contrattuale e sulla manualistica per l'utenza.

---

[23] Si ritiene inoltre opportuno ricordare che la contrattualistica di servizio dei conservatori accreditati deve, ai sensi del documento dell'AgID "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza", anche rispondere ai requisiti ivi riportati tratti dai documenti "*Audit and certification of trustworthy digital repositories*" (le cui indicazioni sono poi state recepite nello standard ISO 16363-2012) e "*Reference model for an open archival information system*" del *Consultative Committee for Space Data Systems* (CCSDS) e dalle raccomandazioni ETSI TS 101 533-1 V1.1.1 (2011-05).

- Uno degli aspetti più importanti da dettagliare nel contratto o nella manualistica di riferimento riguarda il c.d. hand over (passaggio di consegne) dei documenti e dei metadati ad essi associati, sia all'entrata nel contratto, sia durante la sua vigenza,[24] sia alla sua cessazione, per qualsiasi causa. In particolare, deve essere determinata l'assistenza che l'*outsourcer* deve fornire, i relativi corrispettivi, le modalità e i tempi di traslazione "fisica" degli archivi e dei loro *back-up*, i tempi e le modalità di cancellazione degli archivi presso il fornitore uscente, i formalismi del passaggio di consegne.

– Il tema dell'*hand over* è ovviamente e naturalmente correlato a quello della portabilità degli archivi. A livello teorico, gli archivi configurati secondo il d.p.c.m. 3 dicembre 2013 e, in particolare, quelli gestiti dai conservatori accreditati, dovrebbero essere interoperabili, e questo è uno degli scopi fondamentali per cui le regole tecniche hanno adottato particolari standard. Tuttavia, per tutta una serie di motivi, progettuali o accidentali, la portabilità potrebbe, nei fatti, risultare solo parziale.[25] E' quindi opportuno prevedere le opportune garanzie e tutele contrattuali per una corretta gestione dell'interoperabilità degli archivi.

– In sintesi, quanto meglio e in via dettagliata vengono previsti e regolati i possibili *use-case* correlati alla gestione dell'archivio nella manualistica e nei relativi allegati tecnico-operativi (che comunque devono essere collegati giuridicamente al contratto, come sua parte essenziale ed integrante), tanto meno resterà da determinare in senso contrattualistico più stretto, vale a dire, fondamentalmente, le condizioni generali.[26]

– Qui, come sempre, entrano in gioco elementi determinati, dal punto di vista sostanziale, ovviamente da inquadrare giuridicamente in maniera corretta rispetto allo schema contrattuale adottato, anche dai rapporti di

---

[24] Ad esempio, per una parte dell'archivio.

[25] Ad esempio particolari funzionalità implementate potrebbero non essere immediatamente riproducibili in un altro ambiente, oppure non tutti i metadati, aldilà di quelli minimali previsti dalla normativa, associati ai documenti o ai PdA, potrebbero immediatamente essere elaborabili in un altro contesto sintattico-semantico, etc.

[26] Anche i corrispettivi vengono spesso dettagliati in un apposito documento, essendo il più delle volte correlati a parametri determinati in base a necessità tecnico-operative (canoni di attivazione, tipologie documentarie, spazio-disco, numero di documenti, etc.). Un aspetto a volte non ben focalizzato, contrariamente alla sua rilevanza giuridica, è il momento di maturazione dei corrispettivi o il momento di sospensione o cessazione della loro maturazione.

forza delle controparti: obblighi e responsabilità, e relative limitazioni, garanzie, durata, modificazioni del servizio e del contratto, successione nello stesso, disdetta, recesso, gestione dei vizi del sinallagma funzionale, quantificazioni delle penali, determinazione del foro competente, etc.. Un elemento da monitorare sempre con cura, ponendo anche questo in relazione con lo schema contrattuale adottato, è la possibilità per il fornitore di avvalersi nell'erogazione del servizio di soggetti terzi.

– Un aspetto spesso sottovalutato riguarda la gestione della proprietà dei documenti, in particolare, nei casi di successione nella stessa, anche a livello aziendale o di ente: si tratta di un caso tutt'altro che infrequente, spesso caratterizzato da situazioni di non semplice leggibilità giuridica, e che comporta l'esecuzione di una serie di atti formali di non poca rilevanza, come pure la gestione di periodi di transizione a volte non particolarmente "ordinati" dal punto di vista giuridico.

– In particolare, soprattutto a tutela dell'*outsourcer*, è opportuno prevedere clausole per gestire le casistiche di "sparizione" (si passi il termine a-tecnico, ma volutamente omnicomprensivo di situazioni frequenti e più o meno patologiche che i professionisti ben conoscono) dell'*outsourcee*. E' infatti evidente quanto sia opportuno ordinare e formalizzare le opportune precauzioni per non rimanere detentori, se non addirittura custodi, di documenti di soggetti col quale si sia perso ogni tipo di rapporto relazionale o contrattuale.

– Una ultima annotazione riguarda le regole per la cancellazione[27] dei documenti dall'archivio: tale operazione può essere assolutamente legittima (ad esempio per l'erroneo inserimento in archivio di un documento ad esso estraneo), come pure illegittima, anche penalmente sanzionabile (ad esempio, ma ovviamente non solo, in campo tributario). Le regole per la cancellazione devono quindi essere attentamente stabilite in via contrattuale (o nella manualistica allegata), tenendo comunque presente che una conservazione a norma di legge prevede la piena tracciabilità di tutto quanto viene acquisito e viene estromesso dall'archivio.

---

[27] Non si fa riferimento allo scarto programmato, ad esempio per la decorrenza del termine di conservazione dello specifico documento o di cessazione del contrato, ma alla cancellazione/distruzione di documenti prima di tale termine.

2. SICUREZZA E CONTINUITÀ OPERATIVA DEL SISTEMA DI CONSERVAZIONE[*]

Il quadro normativo di riferimento

Il Codice dell'amministrazione digitale[28](CAD), all'articolo 44, applicabile sia alle pubbliche amministrazioni sia ai privati, prevede che un sistema di conservazione di documenti informatici deve assicurare:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento;

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 dal D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali

Il DPCM 3 dicembre 2013, contenente le Regole tecniche in materia di sistema di conservazione, fornisce ulteriori precisazioni in tema precisando che[29]: il sistema di conservazione assicura, dalla presa in carico dal produttore fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, degli oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

E' evidente che solo un sistema di conservazione sicuro può garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità dei documenti in esso conservati.

---

[*] A cura di Davide Grassano, Dottore Commercialista e Revisore Legale, Gruppo di Lavoro "Dematerializzazione documentale", Commissione Informatica CCIAA e Registro Imprese di Milano ODCEC Milano.

[28] D.Lgs. 7 marzo 2005, n. 82 e successive modifiche.

[29] Art. 3 del DPCM 3 dicembre 2013.

Il DPCM 3 dicembre 2013 entra ancora più in dettaglio prevedendo all'art. 12 una serie di regole specifiche riguardanti la sicurezza dei sistemi di conservazione. Viene richiesto alle pubbliche amministrazioni di predisporre, il piano della sicurezza del sistema di conservazione, nel rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D.Lgs. 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del medesimo decreto, nonché in coerenza con quanto previsto dagli articoli 50 - bis e 51 del CAD e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale.

L'articolo 50 bis del CAD si occupa di continuità operativa e *disaster recovery* mentre l'art. 51 presidia la sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni.

In particolare viene precisato che i documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.[30]

Con riferimento ai soggetti privati il comma 2 dell'art. 12 del DPCM 3 dicembre 2013 specifica quanto segue: i soggetti privati appartenenti ad organizzazioni che già adottano particolari regole di settore per la sicurezza dei sistemi informativi adeguano il sistema di conservazione a tali regole. Gli altri soggetti possono adottare quale modello di riferimento le regole di sicurezza indicate dagli articoli 50-*bis* e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. I sistemi di conservazione rispettano le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Anche gli articoli 8 e 12 del DPCM 13 novembre 2014 inerente le "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici", si occupano di misure di sicurezza da adottare con riferimento all'intero ciclo di vita del documento informatico

[30] Art. 51 comma 2 del D.Lgs. 7 marzo 2005, n. 82 e successive modifiche.

Sicurezza per la gestione dei dati personali

La normativa più rilevante in materia di sicurezza dei dati è il D.Lgs. 30 giugno 2003, n. 196 aggiornato da una serie di specifici provvedimenti e da provvedimenti del garante su trattamenti che riguardano settori o specifiche tipologie di dati che richiedono l'adozione di specifiche misure di sicurezza per il trattamento con sistemi informatici dei dati personali e che devono essere garantiti anche dai sistemi di conservazione che gestiscono tali dati.

L'attuale art 31 del Codice, il quale impone che i dati siano "custoditi e controllati [...] in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". Alcuni di questi obblighi sono esplicitati nell'articolo 34 e nell'allegato tecnico di riferimento B sotto forma di misure minime di sicurezza (intese come "il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta").

Tali misure comprendono:

– autenticazione informatica;

– adozione di procedure di gestione delle credenziali di autenticazione;

– utilizzazione di un sistema di autorizzazione;

– aggiornamento periodico (almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

– protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (strumenti elettronici da aggiornare almeno ogni 6 mesi;

– gli aggiornamenti dei programmi volti a prevenire la vulnerabilità dei sistemi elettronici almeno annualmente);

– adozione di procedure per la custodia di copie di sicurezza (salvataggio dei dati almeno settimanale), il ripristino della disponibilità dei dati e dei sistemi (entro 7 giorni);

– adozione di procedure per la gestione e l'uso di supporti rimovibili;

– adozione di tecniche di cifratura o di codici identificativi per

determinati trattamenti

La normativa privacy è in fase di profonda revisione a livello Ue. La Commissione ed il Consiglio dell'Unione Europea hanno raggiunto l'accordo sul testo del nuovo Regolamento Europeo in materia di privacy, in corso di approvazione formale da parte del Parlamento Europeo. Fra le novità principali si segnalano il rafforzamento dei requisiti di sicurezza, l'obbligo di notificare le violazioni, l'introduzione della figura del *Data Protection Officer*, il principio di *privacy by design*, il rafforzamento del diritto alla cancellazione dei dati.

Sicurezza nell'ambito di transazioni elettroniche

Il tema della sicurezza delle transazioni elettroniche e della modalità di accertamento dell'identità dei soggetti che effettuano le transazioni è stato affrontato a livello Europeo con il Regolamento (UE) N. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato UE, le cui disposizioni normative più rilevanti entreranno in vigore da Luglio 2016.

Il regolamento ha un impatto significativo in termini di requisiti di sicurezza dei sistemi di conservazione in quanto sono ridefinite le modalità delle firme elettroniche basate in particolare su livelli di sicurezza differenziati, e viene istituito un quadro normativo per garantire l'interoperabilità nell'UE delle firme elettroniche e per aumentare la sicurezza delle transazioni effettuate utilizzando Internet.

Nella nuova normativa i livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata.

Il regolamento ridefinisce anche i requisiti di sicurezza relativi ai prestatori di servizi fiduciari che costituisce un aspetto rilevante per gli aspetti correlati ai servizi di dematerializzazione che vengono offerti da operatori. I prestatori di servizi fiduciari qualificati e non qualificati dovranno adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati con un livello di sicurezza commisurato al grado di rischio esistente, tenuto conto degli ultimi sviluppi tecnologici.

Tale aspetto ribadisce un aspetto fondamentale che supera il concetto tradizionale di regole tecniche o misure di sicurezza tradizionali in quanto

le misure non sono solo tecniche ma anche organizzative e il livello di sicurezza deve essere correlato alla analisi e valutazione del rischio esistente. Ulteriore elemento che richiede la creazione di un sistema di gestione della sicurezza è rappresentato dal requisito di adeguamento delle misure di sicurezza agli ultimi sviluppi tecnologici.

Sicurezza dei documenti classificati

Il Decreto del Presidente del Consiglio dei Ministri 6 novembre 2015, comprendente la "Disciplina della firma digitale dei documenti classificati" (Decreto n. 4/2015) e le "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva" (Decreto n. 5/2015), introduce nuovi elementi per la tutela di tali documenti, alla luce dei rischi cibernetici e in relazione alle necessità di protezione dei dati personali. Ne consegue che le disposizioni contenute in questi atti vadano tenute in debito conto, da parte di tutti i soggetti pubblici e privati che gestiscono in via informatizzata questioni coperte da segreto di Stato e informazioni classificate, richiede oltre a diversi requisiti sui documenti da conservare:

– la predisposizione di un Piano per la sicurezza che indirizza vari elementi richiesti quali infrastruttura di sicurezza, servizi, personale addetto, crittografia e cifrature, controlli e contromisure e continuità operativa e altri elementi rilevanti per la tipologia di dati trattati.

– La costituzione di un giornale di controllo costituito dall'insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati.

Regole Tecniche per la gestione e la sicurezza dei sistemi di conservazione e standard di riferimento

Con riferimento alla conservazione dei documenti informatici, l'Allegato 3 al DPCM 3 dicembre 2013 fornisce il seguente elenco di standard e specifiche tecniche, ritenute coerenti con le Regole tecniche del CAD:

– ISO 14721:2002 OAIS (*Open Archival Information System*), Sistema informativo aperto per l'archiviazione.

– ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems – Requirements*, Requisiti di un ISMS

(*Information Security Management System*).

– ETSI TS 101 533-1 V1.1.1 (2011-05) *Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management*, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

– ETSI TR 101 533-2 V1.1.1 (2011-05) *Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors*, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

– UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

– ISO 15836:2003 *Information and documentation - The Dublin Core metadata element set*, Sistema di metadata del Dublin Core.

Come modello di riferimento per la gestione dei sistemi di conservazione, lo standard più significativo, è l'ISO 14721:2002 OAIS.

Il modello OAIS è stato sviluppato originariamente dal *Consultative Committee for Space Data Systems (CCSDS)*, e successivamente recepito e pubblicato come standard ISO 14721. Lo standard ha subito già alcuni aggiornamenti e il prossimo è previsto nel 2017.

Il modello OAIS si limita a definire il quadro architetturale in cui il processo di conservazione si svolge e le funzionalità del sistema di conservazione e si basa su un modello dei ruoli che assume rilevanza anche ai fini della determinazione dei requisiti di sicurezza, individuando i soggetti interessati, destinatari e coinvolti nel processo di conservazione, e le relazioni di questi con il sistema di conservazione. Inoltre specifica chiaramente la struttura degli oggetti da scambiare con il mondo esterno e da conservare.

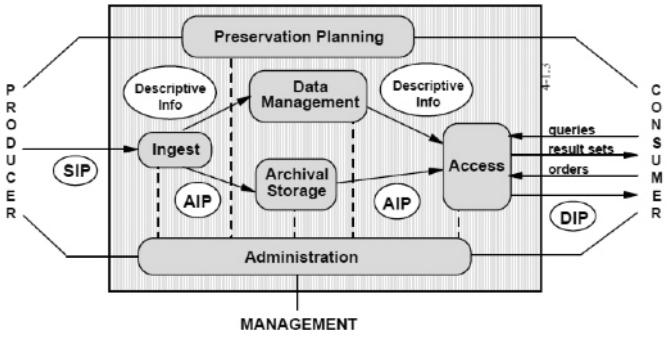
Al centro dell'architettura OAIS vi è la gestione di pacchetti informativi correlati alle esigenze di una comunità di utenti.

L'utente può essere una persona, un ente o un sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse. Nel modello OAIS, gli utenti, tipicamente, vengono raggruppati in community, diversificate per esigenze informative, diritti di accesso alle informazioni, etc.

Un pacchetto informativo è un "contenitore" digitalizzato che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.

Questa visione della struttura dei pacchetti informativi corrisponde al concetto che ogni oggetto digitale, per avere un significato, debba contenere al suo interno due componenti: il *Data Object*, e cioè una sequenza di bit, che di per sé potrebbe non significare nulla, e la *Representation Information* (un insieme di metadati), che specifica le modalità di codifica dell'informazione binaria e ne fornisce quindi l'indispensabile chiave di decodifica e quindi di lettura e di interpretazione. Tale modello favorisce la interoperabilità fra sistemi di conservazione e la creazione di sistemi di gestione dei ruoli federati o ibridi che rispettano gli stringenti requisiti previsti dalle normative di riferimento.

A seguire si presenta un esempio sintetico di schema di architettura OAIS.



Nel dettaglio i pacchetti informativi previsti dal modello si distinguono in base alle diverse fasi di gestione del processo conservativo in *Submission Information Package (SIP)*, che viene trasmesso nella fase di versamento dal produttore al deposito di conservazione; *Archival Information Package (AIP)*, che viene generato a partire dal SIP in fase di accettazione *(Ingestion)* e poi diventa oggetto diretto della conservazione; *Dissemination Information Package (DIP)*, che viene generato a partire dall'AIP per essere distribuito alla Comunità individuata di utenti autorizzati alla sua fruizione.

Le principali figure coinvolte nel sistema di conservazione che devono mettere in atto anche le misure di sicurezza sono:

Il Produttore:

Persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle PA, tale figura si identifica con responsabile della gestione documentale che deve garantire che il sistema documentale che

raccoglie i dati garantisca le misure di sicurezza previste dalla normativa. La gestione dei ruoli e dei profili del produttore è rilevante sia ai fine della tutela dei dati sia per la prevenzione dei reati informatici.

Il Responsabile della conservazione:

Il responsabile della conservazione, è un ruolo determinato nei suoi profili giuridici e funzionali dalla normativa nazionale. In particolare il responsabile della conservazione adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione fra le quali si segnala:la predisposizione del Piano di Sicurezza del sistema di conservazione, il monitoraggio e il controllo della la sicurezza dei sistemi informativi a supporto del Sistema di conservazione, minimizzando il rischio residuo, assicurando la continuità del business e il soddisfacimento dei requisiti relativi alla privacy e alla protezione de dati personali trattati.

Per quanto riguarda la sicurezza di un sistema di conservazione lo standard più significativo proposto nell'Allegato 3 al DPCM 3 dicembre 2013 è l'ISO/IEC 27001:2005

Nel corso dell'ultimo decennio si sono affermati alcuni standard di riferimento per la corretta applicazione della sicurezza. Nell'ambito di tali standard, in particolare, l'ISO 27000, afferma che la Sicurezza delle informazioni si caratterizza nella salvaguardia e protezione di tre parametri fondamentali delle informazioni stesse: la riservatezza, la disponibilità e l'integrità, cui si aggiunge l'autenticità.

Come già esposto in dettaglio nel paragrafo denominato "Il quadro normativo di riferimento" un sistema di conservazione a norma deve possedere le seguenti caratteristiche:

Autenticità:

L'autenticità è la capacità del sistema di conservazione di garantire la provenienza dei documenti conservati.

L'integrità:

Il sistema di conservazione deve consentire un accesso in lettura e non permettere di modificare i documenti conservati.

La affidabilità:

I processi in essere disegnati e sviluppati devono garantire che i documenti non siano alterati nel tempo, e che ci siano sistemi e controlli che assicurano che i documenti non siano persi e che le informazioni gestite dai sistemi di gestione documentale non siano perse o alterate per permettere un regolare svolgimento dei processi relativi. In particolare il ciclo di sviluppo del software deve garantire il mantenimento di attributi dei documenti a prescindere da cambio di ruoli e modelli organizzativi o da cambio di release di software o delle terze parti coinvolte e agli altri

elementi per mantenere nel tempo il processo di gestione e conservazione dei documenti.

La leggibilità:

I processi e le tecnologie adottate devono essere disegnati e sviluppati per garantire che i documenti siano leggibili nel tempo e durante tutto il ciclo di vita, e che informazioni gestite dai sistemi di gestione documentale e conservazione mantengono nel tempo le necessarie funzionalità di ricerca e di accesso ai documenti. La leggibilità deve essere garantita anche in presenza di cambi di tecnologie, modelli, ruoli organizzativi o di terze parti coinvolte nei processi di gestione e conservazione dei documenti.

La reperibilità:

La reperibilità e disponibilità dei documenti sono in qualche modo un requisito aggiuntivo rispetto a quelli precedenti ovvero, il sistema deve garantire livelli di servizio che garantiscono la continuità operativa dei servizi di accesso ai documenti. Inoltre è necessario attivare processi di *business continuity* e *disaster recovery* che garantiscono il rispristino delle funzionalità e dei documenti anche in presenza di eventi accidentali che comportano la mancanza di disponibilità dei sistemi o la perdita anche fisica dei supporti dove sono memorizzati i documenti

Le sopra citate caratteristiche richieste dalla normativa sulla conservazione sono presidiate anche dallo standard ISO 27000, che rimane il più diffuso ed appropriato standard applicabile ai temi della sicurezza informatica.

In particolare, le principali aree indirizzate dello standard ISO 27001 sono:

– I requisiti per la "costruzione" di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) - *Information Security Management System (ISMS)*.

– I requisiti per le misure di sicurezza da implementare in accordo ai bisogni di specifici dell'organizzazione.

– Il processo di valutazione e verifica di conformità che rappresenta la base del funzionamento di un ISMS.

Il concetto di ISMS è mutuato dal mondo della qualità come strumento per tenere sotto controllo (in modo sistematico e nel tempo) i processi legati alla sicurezza, tramite la definizione di ruoli, responsabilità, procedure formali (sia per l'operatività aziendale che per la gestione delle emergenze) e canali di comunicazione. La definizione di un sistema di gestione è di fondamentale importanza nell'ambito della sicurezza in quanto non è sufficiente progettare una soluzione tecnica sicura, ma è

altrettanto importante mantenerne la sicurezza nel tempo. In particolare sono individuate:

– le politiche aziendali (è cioè necessario il coinvolgimento della direzione sia per avere una visione globale e strategica del problema della sicurezza che per dedicare risorse);

– gli atteggiamenti individuali (formazione e sensibilizzazione del personale, creazione di canali di comunicazione).

Collegato al precedente standard vi è l'ISO27002 che rappresenta un set completo di controlli, comprendenti le best practices dell'Information Security.

Altri standard rilevanti presenti nell'Allegato 3 al DPCM 3 dicembre 2013 sono l'ISO 15386 e UNI 11386 Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

L'ISO 15386 *Dublin Core Metadata Initiative*, in acronimo DCMI) si è sviluppato in ambito OCLC (*On line Computer Library Center*), la grande rete di servizi americana per le biblioteche e disciplina l'area dei metadati.

Lo scopo è quello di stabilire un insieme base di elementi descrittivi dell'oggetto digitale, ed inclusi in esso, o da esso referenziati con la definizione di un'architettura per i metadati ad hoc.

Rilevante ai fini della gestione della sicurezza e alle correlazione con un sistema di gestione della identità e dei ruoli sono:

– Autore Entità che ha la responsabilità principale della produzione del contenuto della risorsa. Esempi di Autore possono essere una persona, un'organizzazione o un servizio responsabili del contenuto intellettuale della risorsa.

– Soggetto Argomento principale della risorsa. In particolare un Soggetto può essere espresso da parole o frasi chiave, o da codici di classificazione che descrivono l'argomento della risorsa. Solitamente questi termini vengono scelti tra i valori di un vocabolario controllato o di uno schema di classificazione formale.

– Editore Entità responsabile della pubblicazione della risorsa. Esempi di Editore possono essere una persona, un'organizzazione o un servizio che si occupa di rendere disponibile la risorsa nella sua forma attuale.

– Autore di contributo subordinato Entità responsabile della produzione di un contributo al contenuto della risorsa. Esempi di Autore secondario includono una persona, un'organizzazione o un servizio che contribuiscono alla produzione della risorsa.

Infine lo standard italiano UNI 11386 Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali nell'ambito della

continuità operativa, indirizza il Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali, propone un'architettura informativa che supporti il processo di conservazione sostitutiva necessaria per la creazione di un Indice di Conservazione. Grazie allo standard UNI 11386:2010 SInCRO viene individuato uno schema XML, una struttura dati condivisa da adottare per favorire l'interoperabilità tra i sistemi di conservazione in caso di migrazione.

Manuale di conservazione e sicurezza dei dati

Il manuale di conservazione è il documento fondamentale per la gestione del sistema di conservazione e dei relativi processi.

Il manuale della conservazione è il documento di riferimento in cui vengono descritte in modo dettagliato fasi di lavoro, strumenti e responsabilità che caratterizzano tutta l'attività di conservazione e alcuni aspetti rilevanti per la gestione della sicurezza e deve essere integrato con il sistema di gestione della sicurezza.

Tra le informazioni che devono essere presenti, rilevanti anche ai fini della sicurezza, si segnalano:

– la descrizione della struttura organizzativa e dei soggetti che hanno assunto, nel tempo, la responsabilità del sistema di conservazione, in cui sono esposte funzioni responsabilità e obblighi di chi interviene nel processo di conservazione. Il modello deve tenere conto di un adeguato livello di segregazione delle funzioni e che sia tempestivamente adeguato nel caso di cambiamenti di ruolo.

– la descrizione del processo di conservazione ed il trattamento dei documenti nel sistema di conservazione nel rispetto della normativa sulla protezione dei dati personali; in tale sezione del manuale sono descritti i controlli e il tipo di verifiche effettuate sulla congruità del pacchetto da parte del conservatore e come viene gestito le anomalie tenuto anche conto della tutela prevista dei diritti dell'interessato tutelati dalla normativa.

– le componenti tecnologiche, fisiche e logiche utilizzate, quali le misure di sicurezza relative e come le stesse vengono gestite ed evolute nel tempo incluse le attività di mitigazione dei rischi poste in essere.

– il processo di correzione delle anomalie e come viene svolto il monitoraggio sul corretto funzionamento del sistema di conservazione e sull'integrità dei documenti conservati. In questo ambito va evidenziato il comportamento che andrebbe ad adottarsi in caso anomalie in particolare

in caso di perdita o furto di dati;

– le modalità previste per gestire la continuità dei processi in presenza di eventi imprevisti e le modalità con cui è garantito il ripristino dei processi (*Business Continuity*) e dell'infrastruttura tecnologica necessaria a garantire i processi di conservazione (*Disaster Recovery*).

– la descrizione del sistema dei controlli e delle procedure di monitoraggio della funzionalità del sistema di conservazione e il piano di audit e verifiche sui dati e sui processi di conservazione

Rischi e minacce riguardanti un Sistema di Conservazione

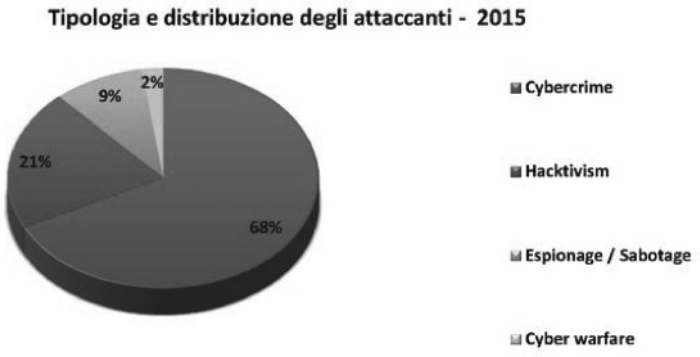
I rischi possono avere varia natura e sono anche legati al contesto operativo di un sistema di conservazione in cui sono gestiti i processi documentali. Esempi di rischi che devono essere normalmente fronteggiati sono a titolo esemplificativo:

- Alterazione dei documenti o dei metadati
- Attacchi su sorgenti/network/sistemi/applicazioni
- Incidenti operazionali, errori, disservizi
- Inaccessibilità dei documenti
- Perdita di documenti, di dati salvati e di metadati
- Perdita o corruzione dei dati in caso di guasto a sistemi o danni fisici
- Furto di documenti
- Perdita di connettività
- Malfunzionamento delle applicazioni o dei servizi
- Accessi non autorizzati ai documenti
- Accesso alle credenziali degli utenti coinvolti nel ciclo di vita dei documenti
- Divulgazione o condivisione della password di utenti del sistema di gestione dei documenti

La *cyber security* è quella pratica che consente a una entità la protezione dei propri *asset* fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal *cyber space*. A sua volta, il *cyber space* viene definito come il complesso ecosistema risultante dall'interazione di persone, software e servizi su Internet per mezzo di tecnologie, dispositivi e reti ad esso connesse.

L'ultimo rapporto CLUSIT disponibile ci fornisce utili indicazioni sulla tipologia di attaccanti e sulle minacce principali.

La tipologia degli attaccanti è sintetizzata nella tabella seguente:



Come ogni rischio aziendale, il rischio *cyber* non può essere eliminato e ha quindi bisogno di un insieme di azioni coordinate per poter essere gestito. Azioni che coinvolgono gli ambiti organizzativi e tecnologici dell'azienda, oltre che di gestione finanziaria del rischio, anche attraverso la definizione di una strategia di gestione del rischio residuo, abilitando in tal modo l'adozione di un approccio integrato di prevenzione del rischio e di protezione del bilancio dell'impresa. Inoltre, il rischio *cyber* è intrinsecamente altamente dinamico. Esso cambia al cambiare delle minacce, delle tecnologie e delle regolamentazioni.

Le più comuni tipologie di minacce analizzate sono:

SQLi:

attacco mirato a colpire le applicazioni web che si appoggiano su un data base. Questo attacco sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una interrogazione dei data base in particolare ai servizi di ricerca e analisi ed estrazione dei dati conservati. Le conseguenze prodotte sono imprevedibili: l'*SQL injection* permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito anche senza essere in possesso delle credenziali d'accesso e di visualizzare e/o alterare dati presenti del database che può rappresentare una componente rilevante del sistema documentale o del sistema di conservazione

DDoS:

Indisponibilità delle informazioni causate da un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio agli utenti del sistema fino a renderlo non più in grado di erogare il servizio ai client richiedenti, tale minaccia è tipica dei siti web e dei sistemi di conservazione che hanno servizi esposti su intenet.

Vulnerabilities:

Attacco ad una componente di un sistema, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente a un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema, in particolare l'attacco ad un sistema secondario può essere usato per accedere al sistema di conservazione ed ad altri sistemi rilevanti nel processo di creazione, versamento e trasmissione dei documenti.

Multiple threats/ATP:

Tipologia di attacco difficile da identificare che, partendo da un attacco mirato, creazione di una *backdoor* dove gli attaccanti cercano di ottenere le credenziali di amministratore del dominio. Gli attaccanti quindi, si muovono "lateralmente" all'interno della rete, installando *backdoor* e *malware* attraverso metodi di "*process injection*", modifiche di registro di sistema o servizi schedulati arrivano a installare una serie di *malware* all'interno delle reti del bersaglio al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni dalle reti del soggetto preso di mira, il furto di dati non viene rilevato se non quale anomalia nei dati in uscita.

Account craking:

gli attaccanti utilizzano applicazioni ad hoc o cercano e identificano le persone che saranno bersaglio degli attacchi e, utilizzando varie fonti e metodi, ottengono i loro indirizzi e-mail o i riferimenti di *instant messaging* per acquisire l'identità elettronica dell'attaccato.

Phishing/ Social Engeniring:

l'attaccante prende di mira utenti specifici all'interno della società target con messaggi di posta elettronica fasulli che contengono link pericolosi o dannosi, oppure file malevoli allegati (PDF o documenti). Questa fase consente di infettare la macchina e dare all'attaccante un accesso. Gli attaccanti successivamente ottengono la maggior parte di informazioni accedendo i sistemi tramite le valide credenziali utente e vengono acceduti anche altri sistemi utilizzando le stesse credenziali e le informazioni ottenute.

Malware:

si riferisce a quella famiglia di software che ha come obiettivo il danneggiamento o l'alterazione, totale o parziale, del funzionamento di un sistema informatico/telematico.

Esistono varie tipologie di Malware quali:

– Pop-up Virus. Un virus è un software, appartenente alla categoria dei *malware*, che è in grado, una volta eseguito, di infettare dei file in modo

da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante *overclocking*, oppure fermando la ventola di raffreddamento.

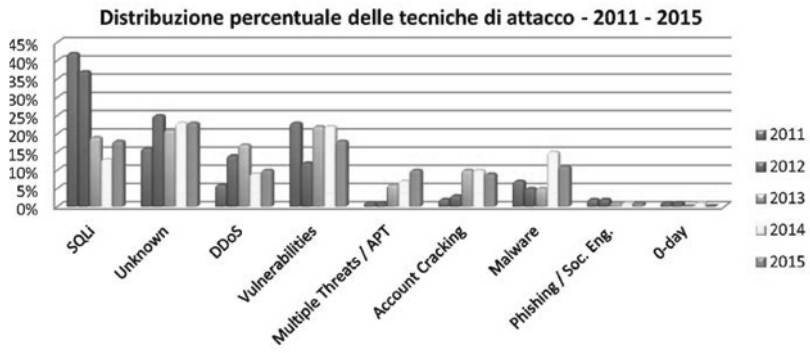
– Pop-up Worm. Un *worm* è una particolare categoria di *malware* in grado di auto replicarsi si riproducono e si copiano di file in file e di sistema in sistema usando le risorse di sistema rallentando il computer.

– Pop-up Spyware. E' un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, ecc.) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.

– Pop-up Trojans. Detti anche "cavalli di Troia" sono dei software che possono rendere vulnerabile l'accesso al sistema infetto.

– Pop-up Keyloggers. Software che registra i tasti premuti dall'utente e li ritrasmette ad un'organizzazione che potrà utilizzarli per trarne profitto, solitamente per furto di identità, catturare password, login, ecc.

Si riporta nella tabella a seguire alcune statistiche disponibili a livello sulla distribuzione della frequenza delle tecniche di attacco sopradescritte:



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia

Il Framework Nazionale di cyber security

I sistemi di conservazione sono esposti ad una moltitudine di attacchi e minacce che sfruttano vulnerabilità dei sistemi informativi e possono

essere sfruttate da un attaccante per entrare illecitamente anche nei sistemi di versamento e conservazione dei dati di una permettendo quindi all'attaccante di leggere, trafugare o cancellare informazioni fino a prendere il controllo informatico del sistema.

Queste vulnerabilità, insieme al fatto che la consapevolezza di questa situazione non è ancora molto elevata, fanno sì che il rischio *cyber* diventi molto rilevante.

In tale contesto è stato sviluppato il *Framework Nazionale di cyber security*[31] il cui scopo è quello di offrire alle organizzazioni un approccio volontario e omogeneo per affrontare la *cyber security* al fine di ridurre il rischio legato alla minaccia *cyber*.

Il modello di *governance* nel *Framework Nazionale di Cyber Security* mette in relazione le caratteristiche specifiche di una organizzazione: pratiche di *Enterprise Risk Management* adottate, standard di sicurezza informatica utilizzati o di cui si ha la certificazione, dimensione della organizzazione e settori produttivi. In particolare, il *Framework*, salendo nel livello di astrazione, agisce da ponte tra strumenti di *Enterprise Risk Management* e *IT & Security Standards*.

Il *framework* prevede l'adozione degli standard richiesti delle normative settoriali come parte integrante dei requisiti di applicazione del *framework*.[32]

Si riporta nella tabella seguente la visualizzazione grafica del frame work nazionale.

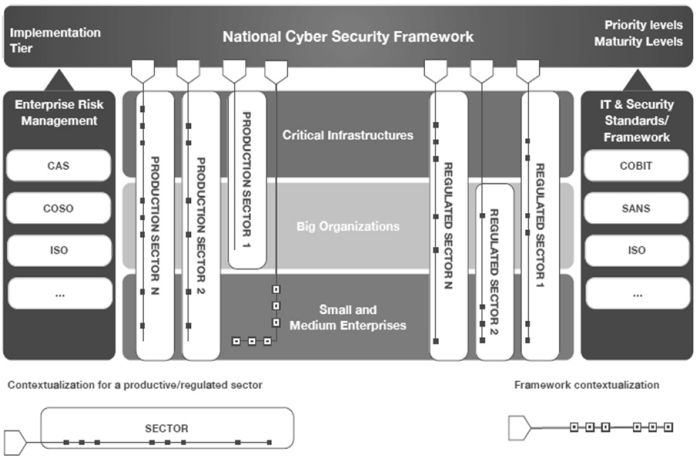
L'approccio di questo *Framework* è intimamente legato a una analisi del rischio e non a standard tecnologici. Il *Framework* è stato specializzato sulla realtà produttiva Italiana. Il *Framework* Nazionale ha come riferimento il *Framework* del NIST[33] a cui aggiunge i livelli di priorità e i livelli di maturità.

---

[31] www.cybersecurityframework.it/.

[32] Ad esempio i soggetti pubblici o privati presenti nell'elenco dei conservatori accreditati *ex* art. 44-*bis* del CAD sono ai sensi della Circolare 65 del 10 aprile tenuti al rispetto dei requisiti di sicurezza contenuti nello standard ISO 27001 e sono soggetti ad una attività periodica di vigilanza da parte dell'AgID, volta ad assicurare che siano mantenuti nel tempo i requisiti che hanno consentito l'iscrizione, pena la revoca dell'accreditamento e la conseguente cancellazione dall'elenco.

[33] Il *National Institute of Standards and Technology (NIST)* è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie e fa parte nel Dipartimento del Commercio e il suo compito è la promozione dell'economia americana attraverso la collaborazione con l'industria al fine di sviluppare standard, tecnologie, e metodologie, che favoriscano la produzione e il commercio.



I livelli di priorità

I livelli di priorità definiscono qual è la priorità con cui si deve affrontare ogni singola *Subcategory del Framework Core*. Da notare che ogni organizzazione è libera di contestualizzare i propri livelli di priorità in base al tipo di *business*, alla dimensione, al suo profilo di rischio.

I livelli di maturità

I livelli di maturità definiscono le diverse modalità con cui si può implementare ogni singola *Subcategory del Framework Core*. Il livello di maturità selezionato deve esser valutato attentamente dalla singola azienda in base al suo *business* e alla sua dimensione nonché al suo profilo di rischio. Tipicamente livelli di maturità maggiori richiedono *effort* maggiore, sia dal punto di vista economico che di gestione. Per alcune *Subcategory* non è possibile definire livelli di maturità.

Il *Framework* opera in una ottica di contestualizzazione dei rischi e la definizione dei relativi livelli di priorità e di maturità. La contestualizzazione dovrà essere fatta rispetto al profilo di *business*, alle vulnerabilità di settore, alla dimensione dell'organizzazione e ad altre caratteristiche aziendali. Una volta che l'organizzazione adotta una contestualizzazione del *Framework*, può calcolare il suo profilo attuale rispetto al rischio *cyber*. Successivamente l'organizzazione dovrà individuare un profilo obiettivo che rispecchia il punto d'arrivo di una strategia aziendale *cyber*.

I tempi e i modi con cui l'organizzazione pianifica il passaggio tra profilo attuale e profilo obiettivo sono di sua pertinenza.

È importante comprendere che il *Framework* non è uno standard di sicurezza, bensì un quadro di riferimento nel quale possono essere inquadrati gli standard e le norme di settore esistenti e future. Il compito di definire gli standard compete agli organi e agli istituti di standardizzazione come l'ISO.

Il *Framework* aiuta l'organizzazione a descrivere il livello di maturità e di rigore delle sue pratiche di gestione del rischio *cyber* una più agevole dimostrazione della applicazione della *"due diligence"*, riferendosi a razionali, oggettivi e misurabili, per aver posto in essere quanto era doveroso attendersi in applicazione del principio di *"duty of care"*. Ogni situazione in cui il corso normale dell'operatività di gestione del ciclo di vita delle informazioni, interrotto o alterato in qualche modo, anche senza conseguenze dirette dannose né potenzialmente in grado di comportare danno alla continuità delle operazioni, è considerata, per definizione, un'anomalia.

Secondo il *Framework Nazionale* con l'evoluzione delle minacce *cyber* è necessario adeguare anche l'approccio alla protezione del patrimonio informativo, delle infrastrutture informatiche e dei processi di *business*, passando da un paradigma statico a una visione dinamica del rischio.

Il *cyber security risk management* è un processo continuo e dinamico, da cui desumere le azioni da implementare per la gestione del rischio in modo consapevole, adeguato agli *asset* da proteggere e in linea, sul piano temporale, con i mutamenti organizzativi, ambientali e tecnologici che coinvolgono l'azienda internamente ed esternamente. In assenza di questo processo, l'azienda rischia di investire e sostenere costi su aree non prioritarie e/o di non investire opportunamente su aree ad alto rischio.

Focalizzandosi sugli scenari di attacco in continua evoluzione, uno dei possibili processi evoluti di gestione del rischio *cyber* viene illustrato di seguito. Esso si basa sull'introduzione di nuove importanti componenti:

Cyber intelligence

Analisi delle minacce nel "mondo reale" attraverso un costante presidio e analisi predittiva di informazioni provenienti da fonti prevalentemente esterne al contesto aziendale. Questa componente di *cyber intelligence* può essere alimentata attraverso un processo di *information gathering*, da fonti istituzionali (CERT, *Intelligence*, Polizia Postale ecc.) e da fonti private (*business information agencies*) che di fatto fungono anche da certificatori della qualità delle informazioni.

Monitoraggio Continuo

Analisi continua delle informazioni provenienti dalle fonti interne al contesto aziendale (ad esempio CERT e SOC), al fine di raffinare e

contestualizzare le probabilità di accadimento degli eventi di minaccia, agendo come fattore abilitante per il calcolo dinamico del rischio.

Threat modelling

Identificazione e selezione dei fattori (minacce, vulnerabilità ed impatti) in grado di rappresentare i potenziali scenari di minaccia, con valutazione dettagliata dei rischi in base alla comprensione delle capacità e delle intenzioni dei potenziali attaccanti.

Information Sharing

Scambio di informazioni rilevanti e tempestive per la prevenzione e/o il contrasto della minaccia *Cyber* verso soggetti governativi (come ad esempio il CERT Nazionale o gli ISAC in USA), pubblici e privati, a valle della definizione di accordi di condivisione.

3. CONSERVAZIONE DIGITALE IN CAMPO CONTABILE E TRIBUTARIO[6]

Introduzione

La conservazione dei documenti contabili e tributari è un'attività che interessa ogni realtà imprenditoriale.

Pare opportuno, prima di entrare nel merito delle disposizioni in materia di conservazione digitale a norma (in passato denominata conservazione sostitutiva) procedere con una panoramica della materia in generale onde definirne il perimetro in cui inserire lo specifico argomento.

Non si può prescindere quindi dall'analisi della disciplina del codice civile racchiusa essenzialmente negli articoli 2215-*bis* e 2220 che si riportano di seguito.

Articolo 2220 codice civile: "Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione. Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti. Le scritture e documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti".

Articolo 2215-*bis* codice civile: "I libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni dell'impresa possono essere formati e tenuti con strumenti informatici. Le registrazioni contenute nei documenti di cui al primo comma debbono essere rese consultabili in ogni momento con i mezzi messi a disposizione

---

[6] A cura di Francesco Milano, Dottore Commercialista e Revisore Legale, Gruppo di Lavoro "Dematerializzazione documentale", Commissione Informatica CCIAA e Registro Imprese di Milano ODCEC Milano.

dal soggetto tenutario e costituiscono informazione primaria e originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

Gli obblighi di numerazione progressiva e di vidimazione previsti dalle disposizioni di legge o di regolamento per la tenuta dei libri, repertori e scritture sono assolti, in caso di tenuta con strumenti informatici, mediante apposizione, almeno una volta all'anno, della marcatura temporale e della firma digitale dell'imprenditore o di altro soggetto dal medesimo delegato. Qualora per un anno non siano state eseguite registrazioni, la firma digitale e la marcatura temporale devono essere apposte all'atto di una nuova registrazione e da tale apposizione decorre il periodo annuale di cui al terzo comma. I libri, i repertori e le scritture tenuti con strumenti informatici, secondo quanto previsto dal presente articolo, hanno l'efficacia probatoria di cui agli articoli 2709 e 2710 del codice civile. Per i libri e per i registri la cui tenuta è obbligatoria per disposizione di legge o di regolamento di natura tributaria, il termine di cui al terzo comma opera secondo le norme in materia di conservazione digitale contenute nelle medesime disposizioni".

In ambito fiscale, la questione della conservazione delle scritture contabili obbligatorie e della relativa documentazione viene affrontata dal combinato disposto normativo degli articoli 22 del d.p.r. 600/1973 e 39 del d.p.r. 633/1972 che si riproducono di seguito per comodità di analisi.

Articolo 22 del d.p.r. 600/1973: "Fermo restando quanto stabilito dal codice civile per il libro giornale e per il libro degli inventari e dalle leggi speciali per i libri e registri da esse prescritti, le scritture contabili di cui ai precedenti articoli, ad eccezione delle scritture ausiliarie di cui alla lettera c) e alla lettera d) del primo comma dell'articolo 14, devono essere tenute a norma dell'articolo 2219 del codice stesso e numerate progressivamente in ogni pagina, in esenzione dall'imposta di bollo. Le registrazioni nelle scritture cronologiche e nelle scritture ausiliarie di magazzino devono essere eseguite non oltre sessanta giorni. Le scritture contabili obbligatorie ai sensi del presente decreto, di altre leggi tributarie, del codice civile o di leggi speciali devono essere conservate fino a quando non siano definiti gli accertamenti relativi al corrispondente periodo di imposta, anche oltre il termine stabilito dall'art. 2220 del codice civile o da altre leggi tributarie, salvo il disposto dall'art. 2457 del detto codice. Gli eventuali supporti meccanografici, elettronici e similari devono essere conservati fino a quando i dati contabili in essi contenuti non siano stati stampati sui libri e registri previsti dalle vigenti disposizioni di legge. [..]"

Articolo 39 del d.p.r. 633/1972: "[…] I registri previsti dal presente

decreto, compresi i bollettari di cui all'articolo 32, devono essere tenuti a norma dell'articolo 2219 del codice civile e numerati progressivamente in ogni pagina, in esenzione dall'imposta di bollo. È ammesso l'impiego di schedari a fogli mobili o tabulati di macchine elettrocontabili secondo modalità previamente approvate dall'Amministrazione finanziaria su richiesta del contribuente. I contribuenti hanno facoltà di sottoporre alla numerazione e alla bollatura un solo registro destinato a tutte le annotazioni prescritte dagli articoli 23, 24 e 25, a condizione che nei registri previsti da tali articoli siano indicati, per ogni singola annotazione, i numeri della pagina e della riga della corrispondente annotazione nell'unico registro numerato e bollato. I registri, i bollettari, gli schedari e i tabulati, nonché le fatture, le bollette doganali e gli altri documenti previsti dal presente decreto devono essere conservati a norma dell'articolo 22 del decreto del Presidente della Repubblica 29 settembre 1973, n. 600. Le fatture elettroniche sono conservate in modalità elettronica, in conformità alle disposizioni del decreto del Ministro dell'economia e delle finanze adottato ai sensi dell'articolo 21, comma 5, del decreto legislativo 7 marzo 2005, n. 82. Le fatture create in formato elettronico e quelle cartacee possono essere conservate elettronicamente. Il luogo di conservazione elettronica delle stesse, nonché dei registri e degli altri documenti previsti dal presente decreto e da altre disposizioni, può essere situato in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza. Il soggetto passivo stabilito nel territorio dello Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, compresi quelli che garantiscono l'autenticità e l'integrità delle fatture di cui all'articolo 21, comma 3, siano stampabili e trasferibili su altro supporto informatico".

Il D.M.E.F. 17/06/2014: conservazione digitale a norma in ambito tributario

Sia il codice civile che la normativa tributaria di cui al testo IVA prevedono quindi la possibilità di poter formare e conservare in modalità elettronica la documentazione contabile e tributaria.

Il riferimento normativo sia per la formazione che per la conservazione elettronica dei documenti siano essi di natura tributaria o civilistica sono il Codice dell'Amministrazione Digitale (CAD), D.Lgs. 7/03/2005 n. 82, e il recente d.m.e.f. 17/06/2014. In quest'ultimo provvedimento si notano molteplici richiami al CAD a partire (articolo 1)

dal rimando alle definizioni dello stesso.

Si ripercorre di seguito il testo del d.m.e.f. 17/06/2014 onde procedere ad una disamina della normativa speciale tributaria.

L'articolo 2 del d.m.e.f. 17/06/2014, che titola "Obblighi da osservare per i documenti informatici", al primo comma opera il rimando alle regole tecniche di cui all'articolo 71 del CAD per la:

- la formazione,
- l'emissione,
- la trasmissione,
- la conservazione,
- la copia,
- la duplicazione,
- la riproduzione,
- l'esibizione,
- la validazione temporale
- la sottoscrizione

dei documenti informatici ai fini tributari.

Proseguendo nella lettura del successivo comma 2 dell'articolo 2 del d.m.e.f. 17/06/2014 sono evidenziate, ancora attuando un rinvio al CAD ed alle relative regole tecniche, le caratteristiche che il documento informatico rilevante ai fini tributari deve necessariamente presentare, ed in particolare:

- immodificabilità,
- integrità,
- autenticità,
- leggibilità,
- formati utilizzabili, anche ai fini dell'accesso agli stessi nel tempo (eventualmente anche individuati in base a scelte motivate dal responsabile della conservazione ed elencati nel manuale di conservazione).

Il successivo articolo 3 del d.m.e.f. 17/06/2014 (Conservazione dei documenti informatici, ai fini della loro rilevanza fiscale) è evidente fin dalla lettura del titolo l'importanza dell'aspetto trattato, in quanto la certezza di effettuare una conservazione digitale a norma, ai fini fiscali, è una condizione essenziale per l'operatore economico che in caso contrario potrebbe vedersi disconoscere la validità giuridica della propria documentazione con esiti sanzionatori evidentemente anche molto significativi.

Al primo comma dell'art. 3 viene detto che la i documenti sono conservati in modo che rispettino due caratteristiche fondamentali.

"a) Siano rispettate le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità".

È quindi evidente che la conservazione dei documenti a rilevanza tributaria è un processo che non può estrarsi esclusivamente dal contenuto endogeno del d.m.e.f. 17/06/2014 ma che, al contrario, richiede un intervento interpretativo e di coordinamento della normativa di rinvio, materia di tipica competenza dei Commercialisti e dei Revisori Legali.

Le norme civilistiche e fiscali trovano la loro armonizzazione nell'integrazione con il corpus di norme in materia di conservazione elettronica che ne detta le linee generali e le regole tecniche.

"b) Siano consentite le funzioni di ricerca e di estrazione delle informazioni dagli archivi informatici in relazione almeno al cognome, al nome, alla denominazione, al codice fiscale, alla partita IVA, alla data o associazioni logiche di questi ultimi, laddove tali informazioni siano obbligatoriamente previste. Ulteriori funzioni e chiavi di ricerca ed estrazione potranno essere stabilite in relazione alle diverse tipologie di documento con provvedimento delle competenti Agenzie fiscali".

Detta seconda caratteristica va a superare in termini di facilità di ricerca la conservazione tradizionale sui supporti cartacei localizzati in strutture fisiche e tangibili; infatti la ricerca cartacea è di gran lunga più macchinosa e lenta oltre che faticosa rispetto alla consultazione di archivi informatici, per cui i moderni sistemi di ricerca permettono di evidenziare le occorrenze di interesse fra decine di migliaia di dati in pochi secondi e offrono quindi la possibilità di una consultazione più veloce ed agevole.

Alla luce di quanto evidenziato la conservazione digitale a norma, se è vero che da un lato implica taluni specifici adempimenti, dall'altro può essere interpretata come è un'opportunità, che permette un notevole miglioramento dell'efficienza del sistema contabile, consentendo anche il conseguimento di ampi margini di risparmio, in particolare quando i volumi documentali siano di importante entità.

Il processo di conservazione termina secondo quanto previsto nel terzo comma del articolo 3 del d.m.e.f. 17/06/2014 con l'apposizione di un riferimento temporale, opponibile ai terzi sul pacchetto di archiviazione onde garantirne l'immodificabilità e quindi l'integrità nel tempo.

Infine all'ultimo comma dell'articolo viene posto il termine entro cui effettuare il processo di conservazione che è quello di cui all'art. 7, comma 4-*ter*, del decreto-legge 10 giugno 1994, n. 357, convertito con modificazioni dalla legge 4 agosto 1994, n. 489 ovvero i "canonici" 3 mesi dalla presentazione della dichiarazione, questo anche per le fatture

elettroniche per le quali era previsto, dall'abrogato d.m.e.f. 23/01/2004, il termine di 15 giorni per il completamento dell'operazione di conservazione sostitutiva.

L'articolo 4 del d.m.e.f. 17/06/2014 si occupa degli "Obblighi da osservare per la dematerializzazione di documenti e scritture analogici rilevanti ai fini tributari". In altri termini è l'articolo che consente di trasformare la documentazione cartacea in documentazione digitale mantenendone il pieno valore giuridico-tributario.

In generale l'articolo 4 si occupa della generazione di copie informatiche e di copie per immagine di documenti e scritture analogici, mentre il processo di conservazione rimane quello previsto dal precedente articolo 3.

Si sottolinea che la regola generale (comma 1) per la digitalizzazione del documento analogici prevede che la generazione della copia informatica o della copia per immagine sia completata con l'apposizione "della firma elettronica qualificata, della firma digitale ovvero della firma elettronica basata sui certificati rilasciati dalla Agenzie fiscali".

Tuttavia bisogna prestare attenzione al fatto che al successivo comma 2 del medesimo articolo nel caso il documento da digitalizzare sia un documento analogico originale unico viene richiesta l'autenticazione da parte di un notaio o di un pubblico ufficiale a ciò autorizzato. È quindi opportuno ricordare la definizione di documento unico che si trae, per procedimento inverso, dalla definizione di documento non unico di cui all'articolo 1 lettera v) del CAD: "v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi".

Ai sensi del primo comma dell'articolo 5 del d.m.e.f. 17/06/2014 della scelta di conservazione digitale, di documenti a rilevanza tributaria, il contribuente deve dare comunicazione nella dichiarazione dei redditi relativa al periodo d'imposta di riferimento.

L'articolo 5 del d.m.e.f. 17/06/2014, al secondo comma, disciplina l'esibizione del documento informatico in caso di verifiche, controlli o ispezioni. In particolare viene specificato che il documento informatico debba essere reso leggibile (in quanto la conservazione digitale potrebbe implicare la non immediata consultabilità del documento) e, a richiesta, disponibile su supporto cartaceo o informatico presso la sede del contribuente ovvero presso il luogo di conservazione delle scritture dichiarato dal soggetto ai sensi dell'art. 35, comma 2, lettera d), del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633.

Si segnala che ad oggi non sono ancora stati emanati i provvedimenti di cui ai commi 3 e 4.

L'articolo 6 del d.m.e.f. 17/06/2014, affronta poi il tema della modalità per l'applicazione dell'imposta di bollo sui documenti informatici che evidentemente non potrà che essere di tipo virtuale con versamento da eseguirsi esclusivamente in via telematica.

Si presi attenzione al fatto che il comma 2 dell'articolo 6 prevede particolari modalità di assolvimento dell'imposta per i documenti informatici, differenziando quindi l'applicazione dell'imposta virtuale rispetto ai documenti cartacei.

Quindi, dall'entrata in vigore del d.m.e.f. 17/06/2014, ovvero dal 26/06/2014, si può schematizzare come segue l'attuale quadro di riferimento per l'assolvimento dell'imposta di bollo e relativi adempimenti correlati.

Per fatture, atti, documenti e registri emessi o utilizzati durante l'anno:

– pagamento: a consuntivo mediante modello F24, entro 120 giorni dalla chiusura dell'esercizio;

– comunicazione: con l'entrata in vigore del d.m.e.f. 17/06/2014 è stata abrogata la comunicazione preventiva e consuntiva prevista dal precedente d.m.e.f. 23/01/2004;

– acconti: con la normativa in vigore non sono previsti acconti;

– fatture elettroniche: devono riportare specifica annotazione di assolvimento dell'imposta ai sensi del d.m.e.f. 17/06/2014;

– bollo su libri e registri: l'imposta deve essere corrisposta per ogni 2.500 registrazioni o frazioni di esse invece che in ragione delle 100 pagine previste per i documenti cartacei.

In base all'ultimo punto si può rilevare che per libri e registri di una certa consistenza vi sia la possibilità di conseguire un notevole risparmio d'imposta rispetto al supporto cartaceo in ragione del fatto che la stessa venga calcolata per registrazioni e non per righe.

Regole tecniche di conservazione digitale a norma

Si è più volte fatto notare come il d.m.e.f. 17/06/2014 operi numerosi rinvii alle regole tecniche richiamate dall'articolo 71 del CAD (Codice dell'Amministrazione Digitale).

Tra le diverse regole tecniche alle quale si riferisce il suddetto articolo 71, ai nostri fini, le più rilevanti per l'implementazione di processi di conservazione digitale a norma ai fini tributari sono:

– d.p.c.m. 3/12/2013: 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 non confondere con il d.p.c.m. 3/12/2013: "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").

Il d.p.c.m. 3/12/2013 va a sostituire, nei termini previsti dall'articolo 14, le previgenti norme tecniche previste dalla Deliberazione del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) del 19 febbraio 2004 n. 11.

– d.p.c.m. 13/11/2014: Decreto del Presidente del Consiglio dei Ministri 13/11/2014, "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".

Il responsabile della conservazione

Figura chiave per la gestione del processo di conservazione risulta essere il responsabile della conservazione i cui compiti sono stati ridelineati dall'articolo 7 del d.p.c.m. 3/12/2013.

Dal punto di vista tributario, successivamente all'entrata in vigore del d.p.c.m. 3/12/2013, non si sono ancora avute espressioni interpretative da parte dell'amministrazione finanziaria circa tale ruolo e sul soggetto che lo debba rivestire.

Può essere opportuno, comunque, richiamare quanto espresso dall'Agenzia delle Entrate con la Circolare 36/2006, tuttavia ancora in vigenza della Deliberazione del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) del 19 febbraio 2004 n. 11: "Il responsabile della conservazione di norma si identifica con il contribuente, salva la facoltà di quest'ultimo di designare un terzo; nel caso di contribuenti diversi dalle persone fisiche, spetta agli stessi il potere di nominare il responsabile della conservazione che potrà essere sia un soggetto legato da un rapporto qualificato (un socio o un amministratore) sia un terzo esterno alla società, all'associazione o all'ente".

4. LA TENUTA DELLA CONTABILITÀ E LA CONSERVAZIONE DEI DOCUMENTI CONTABILI E FISCALI ALL'ESTERO(*)

Premessa

Il mercato economico italiano rileva la presenza di numerose società appartenenti a Gruppi internazionali operanti nel nostro Paese. La recente crisi mondiale ha indotto tali organizzazioni a valutare e adottare nuovi modelli di business con visione più globale che, in molti casi, hanno portato a delocalizzare in altri Stati le funzioni di natura operativa e/o a centralizzare quelle di supporto alle attività principali.

Tra queste ultime rientrano le funzioni amministrative, ed è questo il tema che intendiamo affrontare con la presente ricerca, confrontandoci con le disposizioni normative relative alla tenuta e conservazione dei documenti, dei registri e dei libri contabili.

Con l'incarico di professionisti, in diversi casi ci siamo sentiti rivolgere sicuramente le domande: "È possibile tenere la contabilità della nostra società all'estero?", "È possibile conservare i documenti contabili all'estero?", "Possiamo non stampare le fatture emesse?". A questi quesiti vorremmo cercare di dare risposta alla fine di quest'analisi, come se stessimo dialogando con i nostri clienti.

I documenti presi in esame

Il sistema di contabilità italiano prende in considerazione due principali serie di libri (abbiamo omesso quei libri imposti da altre leggi specifiche

(*) A cura di Ruggiero Delvecchio, Dottore Commercialista e Revisore Legale, Segretario Gruppo di Lavoro "Dematerializzazione documentale", Commissione Informatica CCIAA e Registro Imprese di Milano ODCEC Milano.

quali il lavoro, l'ambiente, ecc.) così come previsto dalla normativa civilistica e fiscale.

Nello specifico, il codice civile italiano richiede:

- il "Libro Giornale", su cui devono essere registrate tutte le operazioni societarie in rigoroso ordine cronologico ai sensi dell'art. 2216 Codice Civile;
- il "Libro Inventari", redatto alla fine di ciascun esercizio finanziario, che deve contenere, in particolare, una descrizione e valutazione di tutte le attività e passività. L'inventario si chiude con lo stato patrimoniale e il conto economico, che deve indicare chiaramente e con fedeltà i profitti ottenuti o delle perdite subite (art. 2217 c.c.);
- che siano tenute le altre scritture contabili richieste dalla natura e dalle dimensioni dell'impresa e, che siano conservate ordinatamente per ciascun affare gli originali delle lettere, dei telegrammi e delle fatture ricevute, nonché le copie delle lettere, dei telegrammi e delle fatture spedite (art. 2214 cc.); tra le altre scritture contabili necessarie per l'esecuzione dell'attività si classificano, ad esempio, il piano dei conti, le schede di contabilità generale, i dati relativi alle immobilizzazioni, i registri IVA ecc., anche se considerati complementari e/o di origine fiscale, sono valutati come parte del sistema di contabilità generale.

La normativa fiscale, così come disposto dal D.P.R. n. 600 / 1973, prevede che siano tenuti e conservati anche i seguenti documenti:

- il registro dei beni ammortizzabili (art. 16 DPR 600/1973);
- i registri IVA così come regolamentati dal DPR 633/1972;
- i dati di supporto al trattamento delle ritenute d'acconto;
- ogni altro dato e/o documento relativo al sistema contabile, sia esso manuale o computerizzato.

I sistemi gestionali internazionali

Per rendere più chiare le nostre argomentazioni, è opportuno fare un veloce cenno ai motivi che hanno portato i Gruppi internazionali a dotarsi di sistemi gestionali capaci di far interagire tra loro utenti di diversi Paesi appartenenti allo stesso Gruppo.

Tali applicativi sono stati implementati per affrontare in modo sistematico le esigenze di natura gestionale, contabile, amministrativa, logistica con l'intento di armonizzare le differenze presenti a livello di singolo Paese e assicurare in capo alla Casa Madre una chiave di lettura congrua e coerente dei dati, ad esempio in termini di principi contabili,

valuta, lingua, etc. e, allo stesso tempo consentire di automatizzare alcuni processi concernenti le transazioni che avvengono all'interno di uno stesso Gruppo.

Si può solo immaginare quale possa essere stato lo sforzo iniziale richiesto per avviare simili organizzazioni in termini di risorse dedicate per l'analisi, lo sviluppo, la formazione, dando origine a investimenti molto rilevanti.

Anche la successiva manutenzione di tali sistemi gestionali si è dimostrata particolarmente onerosa: basti pensare a tutte le modifiche normative che sono apportate periodicamente nei singoli Stati che richiedono un tempestivo adeguamento dei processi in essere, al fine di garantire costantemente la congruità e la coerenza dei dati raccolti a livello centralizzato.

La continua ricerca di massimizzare il profitto nonché la recente crisi economica hanno contribuito a velocizzare i successivi passaggi di razionalizzazione dei processi gestionali orientati a centralizzare alcune funzioni, quali ad esempio quella contabile e amministrativa che ci riguardano più da vicino.

Poiché l'Italia è considerato un Paese "difficile" dal punto di vista burocratico e, allo stesso tempo costoso in termini di gestione delle risorse umane e fiscali, difficilmente si è assistito ad una "centralizzazione" in Italia di tali servizi. Ciò, ha invece causato la chiusura d'interi reparti contabili e amministrativi delle società italiane appartenenti a tali Gruppi con conseguente trasferimento della tenuta della contabilità a soggetti non necessariamente italiani e, ha sollevato tra gli esperti alcuni dubbi e quesiti.

- Cosa vuol dire tenere all'estero la contabilità di una società italiana? È possibile?
- È possibile conservare all'estero i documenti contabili, i registri, i libri e ogni materiale a supporto?
- I processi gestionali implementati saranno sufficienti a garantire l'attendibilità del sistema contabile tenuto all'estero?
- Quali sono i rischi per gli amministratori italiani?

Il quadro normativo di riferimento

L'art. 35, comma 2 - lettera d) DPR 633 / 1972 riguardante la disposizione regolamentare concernente le dichiarazioni di inizio, variazione e cessazione di attività, riporta che «… Dalla dichiarazione di

inizio attività devono risultare … il luogo o i luoghi in cui sono tenuti e conservati i libri, i registri, le scritture e documenti prescritti dal presente decreto e da altre disposizioni…» e le eventuali variazioni devono essere comunicate entro 30 giorni ad uno degli uffici indicati al comma 1 dello stesso articolo normativo.

A tal riguardo si ricorda che per i soggetti diversi dalle persone fisiche, l'Agenzia delle Entrate ha istituito il modello AA7/10 per poter presentare la domanda di attribuzione del numero di codice fiscale e la dichiarazione di inizio attività, la variazione dei dati o la cessazione dell'attività ai fini iva. Sullo stesso è possibile compilare anche il quadro relativo ai luoghi di conservazione delle scritture contabili e, in particolare, la prima sezione richiede che siano comunicati i riferimenti del depositario e il luogo o i luoghi in cui sono conservate le scritture contabili non prevedendo un paese estero e facendo coincidere il concetto di "conservazione" con quello di "tenutario" delle scritture contabili. La seconda sezione è stata predisposta specificatamente per comunicare i luoghi di conservazione delle fatture elettroniche all'estero, così come previsto dall'art. 39 del DPR 633/1972. Non e prevista una sezione per l'indicazione del soggetto che conserva le sole fatture elettroniche in Italia.

L'art. 39, comma 3 DPR 633/1972[34], relativo alla tenuta e conservazione dei registri e dei documenti si esprime come segue: «… Le fatture create in formato elettronico e quelle cartacee possono essere conservate elettronicamente. Il luogo di conservazione elettronica delle stesse, nonché dei registri e degli altri documenti previsti dal presente decreto e da altre disposizioni, può essere situato in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza. Il soggetto passivo stabilito nel territorio dello

[34] L'articolo 39 del D.P.R. 633/72 è stato modificato dal Decreto Legislativo 20 febbraio 2004, n. 52 art. 2, che ha modificato il terzo comma.

Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, compresi quelli che garantiscono l'autenticità e l'integrità delle fatture di cui all'art. 21, comma 3, siano stampabili e trasferibili su altro supporto informatico.»

In attuazione di tale disposizione e stato emanato il D.M. 17 giugno 2014 – pubblicato nella G.U. del 26 giugno 2014 e recante le "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005" – con il quale sono state ridefinite le regole vigenti in materia (dettate in precedenza dall'abrogato D.M. 23 gennaio 2004), stabilendo, tra l'altro, che:

- i documenti informatici devono essere conservati in modo tale che «siano rispettate le norme del codice civile, le disposizioni del codice dell'amministrazione digitale e delle relative regole tecniche e le altre norme tributarie riguardanti la corretta tenuta della contabilità» (cfr. l'articolo 3);
- "il contribuente comunica che effettua la conservazione in modalità elettronica dei documenti rilevanti ai fini tributari nella dichiarazione dei redditi relativa al periodo di imposta di riferimento. In caso di verifiche, controlli o ispezioni, il documento informatico e reso leggibile e, a richiesta, disponibile su supporto cartaceo o informatico presso la sede del contribuente ovvero presso il luogo di conservazione delle scritture dichiarato dal soggetto ai sensi dell'art. 35, comma 2, lettera d), del decreto del Presidente della Repubblica 26 ottobre 1972, n. 633. Il documento conservato può essere esibito anche per via telematica secondo le modalità stabilite con provvedimenti dei direttori delle competenti Agenzie fiscali. (...)" (cosi l'articolo 5).

Dal combinato disposto delle norme richiamate emerge:

a) la facoltà di conservare le fatture elettroniche, cosi come le altre scritture contabili, tanto sul territorio nazionale, quanto all'estero, in Paesi con i quali esista uno strumento giuridico che disciplini la reciproca assistenza;

b) l'obbligo di comunicare nella dichiarazione dei redditi che nell'anno di riferimento si e proceduto alla conservazione sostitutiva;

c) in caso di controlli e verifiche, l'obbligo di rendere leggibili e accessibili i documenti (fatture in primis) tanto dalla sede presso cui il contribuente svolge la propria attività, quanto dal diverso luogo in cui gli stessi sono fisicamente collocati, previa apposita dichiarazione da effettuare ai sensi del citato articolo 35, comma 2, lettera d), del D.P.R. n. 633 del 1972.

Evoluzione Storica dell'Art. 39 del D.P. R. 633/1972

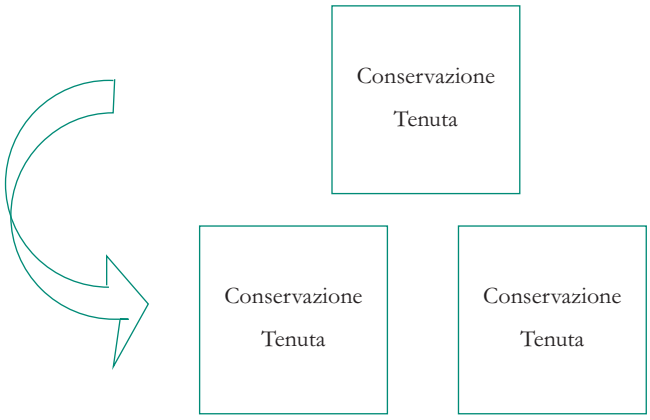
	Art. 39 - Decreto del Presidente della Repubblica del 26/10/1972 n. 633		
	In vigore dal 01/01/2013 *Legge del 24/12/2012 n. 228 Articolo 1*	**In vigore dal 29/02/2004**[35](*) *Decreto legislativo del 20/02/2004 n. 52 Articolo 2*	**In vigore dal 25/10/2001** *Legge del 18/10/2001 n. 383 Articolo 8*
1	I registri previsti dal presente decreto, compresi i bollettari di cui all'articolo 32, devono essere tenuti a norma dell'articolo 2219 del codice civile e numerati progressivamente in ogni pagina, in esenzione dall'imposta di bollo. E' ammesso l'impiego di schedari a fogli mobili o tabulati di macchine elettrocontabili secondo modalità previamente approvate all'Amministrazione finanziaria su richiesta del contribuente. I contribuenti hanno facoltà di sottoporre alla numerazione e alla bollatura un solo registro destinato a tutte le annotazioni prescritte dagli articoli 23, 24 e 25, a condizione che nei registri previsti da tali articoli siano indicati, per ogni singola annotazione, i numeri della pagina e della riga della corrispondente annotazione nell'unico registro numerato e bollato.	I registri previsti dal presente decreto, compresi i bollettari di cui all'articolo 32, devono essere tenuti a norma dell'articolo 2219 del codice civile e numerati progressivamente in ogni pagina, in esenzione dall'imposta di bollo. E' ammesso l'impiego di schedari a fogli mobili o tabulati di macchine elettrocontabili secondo modalità previamente approvate all'Amministrazione finanziaria su richiesta del contribuente. I contribuenti hanno facoltà di sottoporre alla numerazione e alla bollatura un solo registro destinato a tutte le annotazioni prescritte dagli articoli 23, 24 e 25, a condizione che nei registri previsti da tali articoli siano indicati, per ogni singola annotazione, i numeri della pagina e della riga della corrispondente annotazione nell'unico registro numerato e bollato.	I registri previsti dal presente decreto, compresi i bollettari di cui all'articolo 32, devono essere tenuti a norma dell'articolo 2219 del codice civile e numerati progressivamente in ogni pagina, in esenzione dall'imposta di bollo. E' ammesso l'impiego di schedari a fogli mobili o tabulati di macchine elettrocontabili secondo modalità previamente approvate all'Amministrazione finanziaria su richiesta del contribuente. I contribuenti hanno facoltà di sottoporre alla numerazione e alla bollatura un solo registro destinato a tutte le annotazioni prescritte dagli articoli 23, 24 e 25, a condizione che nei registri previsti da tali articoli siano indicati, per ogni singola annotazione, i numeri della pagina e della riga della corrispondente annotazione nell'unico registro numerato e bollato.
2	I registri, i bollettari, gli schedari e i tabulati, nonché le fatture, le bollette doganali e gli altri documenti previsti dal presente decreto devono essere conservati a norma dell'articolo 22 del decreto del Presidente della Repubblica 29 settembre 1973, n. 600.	I registri, i bollettari, gli schedari e i tabulati nonché le fatture, le bollette doganali e gli altri documenti previsti dal presente decreto devono essere conservati a norma dell'art. 22 del decreto del Presidente della Repubblica 29 settembre 1973, n. 600.	I registri, i bollettari, gli schedari e i tabulati nonché le fatture, le bollette doganali e gli altri documenti previsti dal presente decreto devono essere conservati a norma dell'art. 22 del D.P.R. 29 settembre 1973, n. 600.

[34] L'articolo in vigore nel periodo 11/12/2012 - 31/12/2012 per effetto del Decreto Legge del 11/12/2012 n. 216 Articolo 1), è esattamente uguale a quello in vigore dal 29/02/2004.

	Art. 39 - Decreto del Presidente della Repubblica del 26/10/1972 n. 633		
	In vigore dal 01/01/2013 *Legge del 24/12/2012 n. 228 Articolo 1*	**In vigore dal 29/02/2004(*)** *Decreto legislativo del 20/02/2004 n. 52 Articolo 2*	**In vigore dal 25/10/2001** *Legge del 18/10/2001 n. 383 Articolo 8*
3	Le fatture elettroniche sono conservate in modalità elettronica, in conformità alle disposizioni del decreto del Ministro dell'economia e delle finanze adottato ai sensi dell'articolo 21, comma 5, del decreto legislativo 7 marzo 2005, n. 82.	Le fatture elettroniche trasmesse o ricevute in forma elettronica sono archiviate nella stessa forma.	
4	Le fatture create in formato elettronico e quelle cartacee possono essere conservate elettronicamente.	Le fatture elettroniche consegnate o spedite in copia sotto forma cartacea possono essere archiviate in forma elettronica.	
5	Il luogo di conservazione elettronica delle stesse, nonché dei registri e degli altri documenti previsti dal presente decreto e da altre disposizioni, può essere situato in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza.	Il luogo di archiviazione delle stesse può essere situato in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza.	
6	Il soggetto passivo stabilito nel territorio dello Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, compresi quelli che garantiscono l'autenticità e l'integrità delle fatture di cui all'articolo 21, comma 3, siano stampabili e trasferibili su altro supporto informatico.	Il soggetto passivo, residente o domiciliato nel territorio dello Stato assicura, per finalità di controllo, l'accesso automatizzato all'archivio e che tutti i documenti ed i dati in esso contenuti, ivi compresi i certificati destinati a garantire l'autenticità dell'origine e l'integrità delle fatture emesse in formato elettronico, di cui all'art. 21, comma 3, siano stampabili e trasferibili su altro supporto informatico.	

Alcune considerazioni

L'originaria sovrapposizione del concetto di "conservazione" delle scritture contabili con quello di "tenuta" delle stesse, deve necessariamente tenere conto del processo di dematerializzazione dei processi e dei documenti fiscalmente rilevanti.



Guardando anche il processo operativo cartaceo relativo alle scritture contabili, la fase della sola "tenuta" è tale sino a quando le stesse sono state stampate definitivamente sui libri e sui registri per essere conservate.

Al fine di circoscrivere meglio il momento in cui avviene tale cambio di stato è opportuno rifarsi alla normativa, in particolare all'art. 7, comma 4.ter del DL 1994/357[36] che riporta "A tutti gli effetti di legge, la tenuta di qualsiasi registro contabile con sistemi meccanografici è considerata regolare in difetto di trascrizione su supporti cartacei, nei termini di legge, dei dati relativi all'esercizio per il quale i termini di presentazione delle relative dichiarazioni annuali non siano scaduti da oltre tre mesi, allorquando anche in sede di controlli ed ispezioni gli stessi risultino aggiornati sugli appositi supporti magnetici e vengano stampati contestualmente alla richiesta avanzata dagli organi competenti ed in loro presenza."

Per cui il termine di legge entro cui deve essere effettuata la stampa dei libri e dei registri, rappresenta il momento dal quale gli stessi devono essere conservati.

---

[36] Modificato dalla Legge del 24/12/2007 n. 244 Articolo 1.

In ambito digitale, la normativa di riferimento individua, infatti, la figura del "conservatore" classificandolo come colui che effettua il solo processo di conservazione dei documenti fiscali.

In tale processo, infatti, così come definito dal CAD e riportato nel manuale di conservazione, il conservatore e il soggetto delegato ad operare il solo processo di "conservazione elettronica" dei documenti fiscali. Questi può, peraltro:

a) coincidere con il contribuente,

b) assumere la veste del depositario/tenutario (ossia di colui che gestisce la contabilità e che, ai fini fiscali, assume specifiche responsabilità),

c) essere un soggetto terzo.

In tal senso si è espressa l'Agenzia delle Entrate, ritenendo che poiché il conservatore ("elettronico") non e il depositario/tenutario delle scritture contabili, il contribuente non e tenuto a darne comunicazione mediante il modello AA7/10 (essendo, in ogni caso, gli estremi identificativi del conservatore riportati obbligatoriamente nel manuale della conservazione), nel presupposto che, in caso di accesso, i verificatori siano messi in condizione di visionare e acquisire direttamente, presso la sede del contribuente ovvero del "depositario" delle scritture contabili, la documentazione fiscale, compresa quella che garantisce l'autenticità ed integrità delle fatture, al fine di verificarne la corretta conservazione. Va da se che la mancata esibizione dei documenti sopra richiamati comporta gli effetti previsti dagli articoli 39 del D.P.R. n. 600 del 1973 e 52 del D.P.R. n. 633 del 1972.

A modo di vedere dello scrivente, tale processo non si discosta dalle realtà di quelle società che stanno tutt'ora adottando la conservazione cartacea dei documenti contabili, delocalizzando fisicamente gli stessi presso magazzini esterni a cui è stato assegnato tale incarico.

La conservazione elettronica delle fatture emesse in formato elettronico, dei registri e degli altri documenti così come previsto dall'art. 39 DPR 633/1972

L'art. 39, comma 3 del DPR 633/1972 in vigore dal 1° gennaio 2013 ha introdotto una importante novità rispetto al passato, relativa all'opportunità di poter conservare elettronicamente anche i registri e gli altri documenti previsti dallo stesso decreto.

Se ripercorriamo le motivazioni storiche che hanno indotto il legislatore italiano a modificare più volte l'articolo in esame, notiamo che

queste sono strettamente legate al processo di armonizzazione europeo che coinvolge anche il nostro Paese in materia di IVA e, nello specifico, della fatturazione elettronica.

L'enfasi posta dalla Comunità Europea su questo tema è dettata dalla visione condivisa legata ai benefici che derivano dall'adozione della fatturazione elettronica, che sono massimizzati allorché le fatture sono generate, inviate, trasmesse, ricevute ed elaborate in modo completamente automatizzato. Per questo motivo, a tendere, soltanto le fatture leggibili da una "macchina" che possono essere elaborate automaticamente e digitalmente dal ricevente dovrebbero essere considerate conformi alla norma europea sulla fatturazione elettronica; un semplice file di immagini non dovrebbe essere più considerato una fattura elettronica.

Ne emerge quindi un obiettivo di "interoperabilità"[37], che consenta la presentazione e il trattamento delle informazioni in modo uniforme nei diversi sistemi gestionali, indipendentemente dalla tecnologia, dall'applicazione o dalla piattaforma utilizzate. Nello specifico sono state emanate indicazioni per operare su tre livelli distinti: in termini di contenuto della fattura (semantica), formato o lingua usati (sintassi) e metodo di trasmissione.

Tornando alla lettura dell'art. 39, si rileva che il legislatore italiano ha previsto di propria iniziativa anche la conservazione elettronica dei registri e degli altri documenti previsti dal DPR 633/1972[38] oltre a quella della fattura elettronica sulla base delle indicazioni fornite dalla normativa europea. Non sono chiare le motivazioni che hanno indotto il nostro legislatore ad ampliare il campo di azione di tale disciplina; da un lato è apprezzabile la volontà dello stesso di anticipare la soluzione "naturale" e/o più ovvia da un punto di vista procedurale e organizzativo. Per contro, poiché la normativa europea non si è ancora espressa al riguardo, ciò

[37] Direttiva 2014/55/UE del Parlamento Europeo e del Consiglio del 16 aprile 2014 relativa alla fatturazione elettronica negli appalti pubblici.

[38] L'attuale formulazione dell'art. 39, comma 3 del DPR 633/1972 è stata introdotta dall' art. 1, comma 325, lett. f) legge 24 dicembre 2012 n. 228. In effetti, l'art. 39, comma 3 del DPR 633/1972 prevedrebbe la conservazione elettronica nei Paesi esteri con reciproca assistenza anche per registri e documenti previsti da "altre disposizioni". Tale locuzione, a parere di chi scrive, non appare sufficientemente circostanziata e può porre ulteriori dubbi interpretativi con riferimento alla documentazione elettronica non riferita al presente decreto. Peraltro, i provvedimenti attuativi previsti dall'art. 5, comma 3 del D.M.F. 17 giugno 2014, che renderebbero ancora più efficiente la soluzione, non sono stati ancora emanati.

potrebbe generare confusione per quanto riguarda l'applicazione della conservazione elettronica nei Paesi in cui esista uno strumento giuridico che disciplini la reciproca assistenza, se gli stessi non sono preparati in tal senso, sia in termini di adeguamento delle proprie normative che da un punto di vista logistico.

Ciò che risulta estremamente chiaro è la diversità di trattamento dei documenti in formato elettronico rispetto ai documenti cartacei. Questi ultimi, infatti, possono essere conservati solo in Italia, fatta salva l'opportunità di convertire gli stessi in formato digitale.

Ne deriva, di conseguenza, che:

1) qualora la tenuta della contabilità di una società italiana sia affidata a servizi centralizzati localizzati all'estero[39] utilizzando il sistema di conservazione cartaceo, il legale rappresentante della società:

a) è identificato quale "depositario" delle scritture contabili, sebbene si stia avvalendo di servizi di elaborazione dati localizzati all'estero;

b) deve conservare i documenti cartacei in Italia, presso le proprie sedi e/o presso i magazzini esterni a cui sia affidato tale incarico;

c) in caso di accesso delle autorità fiscali, deve fare in modo che i verificatori siano messi in condizione di visionare e acquisire direttamente presso le proprie sedi, la documentazione fiscale, compresa quella che garantisce l'autenticità ed integrità delle fatture, al fine di verificarne la corretta conservazione.

2) qualora la tenuta della contabilità di una società italiana sia affidata a servizi centralizzati localizzati all'estero utilizzando il sistema di conservazione elettronico, il legale rappresentante della società:

a) è identificato quale "depositario" delle scritture contabili, sebbene si stia avvalendo di servizi di elaborazione dati localizzati all'estero;

b) in caso di accesso delle autorità fiscali, deve fare in modo che i verificatori siano messi in condizione di visionare e acquisire direttamente presso le proprie sedi, la documentazione fiscale, compresa quella che garantisce l'autenticità ed integrità delle fatture, al fine di verificarne la corretta conservazione.

---

[39] Abbiamo esaminato nei paragrafi precedenti il caso delle società appartenenti a Gruppi Internazionali.

A parere dello scrivente, il legale rappresentante potrebbe nominare in entrambi i casi un terzo stabilito in Italia, quale depositario delle scritture contabili.

Si riepiloga nella tabella che segue, quanto espresso sopra in merito alla tenuta della contabilità di una società italiana e alla conservazione dei documenti, cartacea o elettronica:

Descrizione	Italia	Estero
Tenuta della contabilità	SI	NO
Conservazione Cartacea	SI	NO
Conservazione Elettronica	SI	SI

La conservazione elettronica nei paesi in cui esista uno strumento giuridico che disciplini la reciproca assistenza

L'art. 39, comma 3 del DPR 633/1972, già nella versione in vigore dal 29 febbraio 2004, aveva introdotto una importante novità rispetto al passato, in merito all'opportunità di poter conservare elettronicamente le fatture elettroniche in un altro Stato, a condizione che con lo stesso esista uno strumento giuridico che disciplini la reciproca assistenza.

A tal riguardo si richiamano, la Direttiva del Consiglio 2011/16/UE del 15 febbraio 2011 relativa alla cooperazione amministrativa nel settore fiscale e, le disposizioni riguardanti lo scambio di informazioni della Convenzione in materia di mutua assistenza amministrativa in campo fiscale, firmata a Strasburgo il 25 gennaio 1988, così come modificata dal protocollo firmato a Parigi il 27 maggio 2010.

Dalle stesse emerge chiaro il messaggio della Comunità Europea di voler affrontare in modo determinato il cambiamento in essere nell'era della globalizzazione, dove la necessità per gli Stati membri di prestarsi assistenza reciproca nel settore della fiscalità si fa sempre più pressante. "La mobilità dei contribuenti, il numero di operazioni transfrontaliere e l'internazionalizzazione degli strumenti finanziari conoscono un'evoluzione considerevole, che rende difficile per gli Stati membri accertare correttamente l'entità delle imposte dovute. Questa difficoltà crescente si ripercuote negativamente sul funzionamento dei sistemi fiscali e dà luogo alla doppia tassazione, la quale di per sé induce alla frode e all'evasione fiscale, mentre i poteri di controllo restano a livello

nazionale. Ne risulta pertanto minacciato il funzionamento del mercato interno.

Per questo motivo uno Stato membro non può gestire il proprio sistema fiscale interno, soprattutto per quanto riguarda la fiscalità diretta, senza ricevere informazioni da altri Stati membri. Per ovviare agli effetti negativi di questo fenomeno è indispensabile mettere a punto una nuova cooperazione amministrativa fra le amministrazioni fiscali dei diversi Stati membri. È necessario disporre di strumenti atti a instaurare la fiducia fra gli Stati membri mediante l'istituzione delle stesse norme e degli stessi obblighi e diritti per tutti gli Stati membri."

La reciproca assistenza tra Stati prevede lo scambio automatico di informazioni riguardati gli individui, le imprese, i redditi, le transazioni bancarie, ecc., e in relazione a casi particolari può essere presentata una richiesta di autorizzazione per i funzionari fiscali affinché possano essere presenti durante una verifica sul territorio dell'altro Stato. In particolare, si tratta di:

1. casi in cui esistono indicazioni di irregolarità transfrontaliere o di evasione fiscale;
2. casi complessi per cui è auspicabile la presenza di funzionari fiscali;
3. casi in cui la presenza dei funzionari fiscali possa accelerare i tempi per effettuare la verifica;
4. verifiche condotte in sede bilaterale o multilaterale;
5. altri casi se autorizzati dalle rispettive Autorità.

Al fine di verificare l'aggiornamento degli accordi e delle convenzioni di reciproca assistenza amministrativa tra Stati per quelli sottoscritti particolari quelli sottoscritti dal Ministero dell'Economia e delle Finanze, si suggerisce di accedere al sito del Dipartimento delle Finanze italiano[40] "MEF".

Considerazioni finali

La tenuta della contabilità e la conservazione dei documenti contabili e fiscali sono stati argomenti oggetto di particolare attenzione da parte del

[40] http://www.finanze.it/opencms/it/fiscalita-comunitaria-e-internazionale/convenzioni-e-accordi/.

legislatore negli ultimi 15 anni e ciò, forse, non accadeva dai tempi dell'introduzione dei pilastri della normativa fiscale italiana quali, ad esempio il D.P.R. 633 / 1972 e il D.P.R. 600 / 1972. Spinto, ovviamente, dall'evoluzione tecnologica e dai conseguenti processi di "dematerializzazione" del sistema cartaceo che stanno coinvolgendo i Paesi più strutturati e, nel nostro caso, la Comunità Europea.

Possiamo dire che questa rivoluzione è appena cominciata e porterà sicuramente altre novità importanti nei prossimi anni, volte a migliorare e a superare i dubbi e le perplessità sopra esposte, aprendo, forse definitivamente quei confini determinati da regole specifiche[41] e da comportamenti non scritti che condizionano tutt'oggi i sistemi contabili di ciascun Paese.

Pensiamo al nostro caso italiano, dove, oltre ai requisiti minimi previsti dal punto di vista civilistico e fiscale per un sistema contabile, come sopra esposto, sono richiesti altri adempimenti specifici (ad esempio lo "Spesometro") che non trovano sempre una reciproca corrispondenza nell'ambito della Comunità Europea.

Per quanto riguarda il sistema di conservazione digitale a norma, si segnala la difficoltà oggettiva di spiegare ad operatori internazionali che i documenti archiviati nei propri applicativi gestionali non costituiscono di per sé un sistema tale e sufficiente per poter garantire la corretta applicazione della normativa Italiana. Come già sopra riportato, il nostro legislatore ha introdotto la regolamentazione della conservazione elettronica, pur non essendo stata prevista dalle direttive della Comunità Europea e ciò, pur trattandosi di una importante soluzione e opportunità, genera in realtà confusione di comprensione da parte degli altri Paesi Europei. Si ritiene, pertanto, che la possibilità data dal nostro legislatore di poter archiviare in altri Stati, a condizione che con gli stessi esista uno strumento giuridico che disciplini la reciproca assistenza, sia difficilmente praticabile per le difficoltà oggettive da parte degli operatori esteri di comprendere, adattare, manutenere e gestire un sistema di conservazione elettronica dei documenti contabili e fiscali conforme alla normativa italiana.

---

[41] In alcuni Paesi della Comunità Europea, ad esempio, la data di registrazione è sostituita dal periodo/mese di riferimento; oppure, il numero di registrazione non deve essere necessariamente progressivo rispetto alla data.

5. IL REGOLAMENTO EIDAS: SCENARI E INDICAZIONI OPERATIVE[*]

Oggetto e ambito di applicazione

Il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio dell'Unione Europea (d'ora in poi il Regolamento), adottato il 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", è stato pubblicato il 28 agosto 2014 nella Gazzetta Ufficiale dell'Unione Europea (Official Journal of the European Union, L. 257).

Il Regolamento, conosciuto anche con l'acronimo eIDAS, *"electronic IDentification Authentication and Signature"*, disciplina in dettaglio:

– le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;

– i servizi fiduciari, in particolare per le transazioni elettroniche;

– l'istituzione di un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Trattandosi di un regolamento comunitario e pertanto come atto legislativo vincolante, deve essere applicato in tutti i suoi elementi nell'intera Unione europea e non vi è necessità, come invece accade con una direttiva, di un recepimento da parte del singolo Stato membro Ue[41] ma è direttamente applicabile in ciascuno degli Stati membri medesimi.

---

[*] A cura di Giuseppe Mantese, Dottore Commercialista e Revisore Legale, Gruppo di Lavoro "Dematerializzazione documentale", Commissione Informatica CCIAA e Registro Imprese di Milano ODCEC Milano.

[41] L'art. 288, par. 2 del Trattato sul funzionamento dell'UE specifica che: "Il regolamento è un atto giuridico avente portata generale e va considerato obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri."

Con riferimento all'ambito di applicazione, il Regolamento[42]:

1. si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione;
2. non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti;
3. non pregiudica il diritto nazionale o comunitario legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.

Entrata in vigore del regolamento

Il Regolamento è entrato in vigore dal 17 settembre 2014 ma la sua applicabilità presenta un dettagliato scadenziario a più tappe. La maggior parte delle disposizioni si applicano a decorrere dal 1 luglio 2016 ad eccezione di una serie di norme elencate al comma 2 dell'art. 52 del Regolamento medesimo. In particolare:

– alla lettera (a) comma 2 dell'art. 52 sono elencate le disposizioni che sono applicabili dal 17 settembre 2014[43];

– alla lettera (b) comma 2 dell'art. 52 sono elencate le disposizioni che si applicano a decorrere dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3[44], e all'articolo 12, paragrafo 8[45] cioè dal 29 settembre 2015;

---

[42] Art. 2 del Regolamento.

[43] In maggioranza tali disposizioni riguardano l'obbligo in alcuni casi e la facoltà della Commissione europea in altri casi, di adottare atti di esecuzione che devono/possono disciplinare operativamente le materie presidiate dal Regolamento medesimo.

[44] Articolo 8, paragrafo 3 (n.d.r livelli di garanzia dei regimi di identificazione elettronica) del Regolamento: "Entro il 18 settembre 2015, tenendo conto delle norme internazionali pertinenti e fatto salvo il paragrafo 2, la Commissione, mediante atti di esecuzione, definisce le specifiche, norme e procedure tecniche minime in riferimento alle quali sono specificati i livelli di garanzia basso, significativo e elevato dei mezzi di identificazione elettronici."

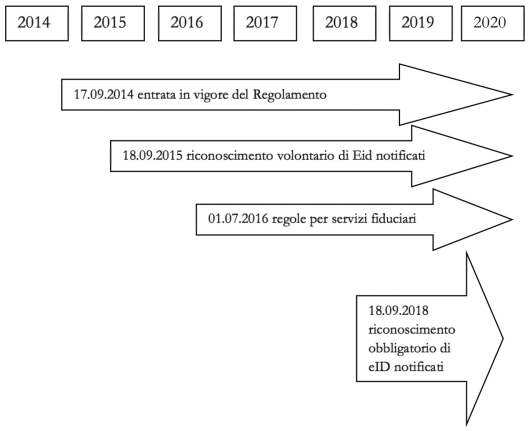
[45] Articolo 12, paragrafo 8 (n.d.r. cooperazione ed interoperabilità) del Regolamento: "Entro il 18 settembre 2015, al fine di garantire condizioni uniformi di esecuzione del requisito di cui al paragrafo 1 (n.d.r. interoperabilità), la Commissione, fatti salvi i criteri di cui al paragrafo 3 e tenendo conto dei risultati della cooperazione fra gli Stati membri, adotta atti di esecuzione sul quadro di interoperabilità quale definito al paragrafo 4."

– alla lettera (c) comma 2 dell'art. 52 sono elencate le disposizioni che si applicano a decorrere da tre anni dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8 cioè dal 29 settembre 2018.

Si evidenzia in particolare che l'obbligo di riconoscimento reciproco delle identificazioni elettroniche scatterà nella seconda metà del 2018. Il 1° luglio 2016 sarà invece abrogata la Direttiva 1999/93/CE che attualmente disciplina il quadro comunitario per le firme elettroniche.

Si riassume nella tabella a seguire le principali scadenze della timeline di adozione delle disposizioni del Regolamento.

Eidas- Attuazione regolamento



Correlati al Regolamento, la Commissione europea ha già adottato una serie di atti di esecuzione.[46] Insieme al Regolamento che fornisce un quadro di principi e regole generali, tendenzialmente stabili nel tempo, è stata prevista l'emanazione, da parte della Commissione europea, di una

[46] A livello generale, al considerando (71) del Regolamento si precisa che: "Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione, in particolare per specificare i numeri di riferimento delle norme il cui impiego conferisce una presunzione di adempimento di determinati requisiti stabiliti nel presente regolamento." Alcuni atti di esecuzione sono obbligatori e richiesti espressamente in alcuni specifici articoli del Regolamento. In particolare era richiesto alla Commissione europea di emanare entro il 18 settembre 2015, gli atti di esecuzione indicati agli articoli: 8 paragrafo 3, 12 paragrafo 8, 22 paragrafo 5, 27 paragrafo 5 e 37 paragrafo 5 del Regolamento.

normativa secondaria, nella forma di atti di esecuzione (regolamenti e decisioni di esecuzione), per la definizione di regole tecniche e tecnologiche che possono cambiare periodicamente anche in funzione dell'evoluzione tecnologica ma che devono garantire condizioni uniformi di esecuzione del Regolamento medesimo[47].

In particolare sulla Gazzetta ufficiale dell'Unione europea n. 235 del 9 settembre 2015 sono stati pubblicati i seguenti Regolamenti e Decisioni di Esecuzione:

– Regolamento di esecuzione (UE) 2015/1501 della Commissione, dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

– Regolamento di esecuzione (UE) 2015/1502 della Commissione, dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

– Decisione di esecuzione (UE) 2015/1505 della Commissione, dell'8 settembre 2015 relativo alle specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

---

[47] Al considerando (72) del Regolamento si specifica ulteriormente che "In sede di elaborazione degli atti delegati o di esecuzione, la Commissione dovrebbe tenere debito conto delle norme e delle specifiche tecniche elaborate da organizzazioni e organismi di normalizzazione europei e internazionali, in particolare il Comitato europeo di normalizzazione (CEN), l'Istituto europeo delle norme di telecomunicazione (ETSI), l'Organizzazione internazionale per la standardizzazione (ISO) e l'Unione internazionale delle telecomunicazioni (UIT), al fine di assicurare un livello elevato di sicurezza e interoperabilità dell'identificazione elettronica e dei servizi fiduciari."

– Decisione di esecuzione (UE) 2015/1506 della Commissione, dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Il regolamento in dettaglio

Il Regolamento è in sintesi così strutturato:

Macrosezioni:	Sezioni del Regolamento più significative:	Riferimenti puntuali agli articoli del Regolamento:
Disposizioni generali (dall' art. 1 al 5)	Oggetto Ambito di applicazione Definizioni	1 2 3
Identificazione elettronica (dall' art. 6 al 12)	Livelli di garanzia dei regimi di identificazione elettronica	8
Servizi fiduciari (dall' art. 13 al 45)	Requisiti di sicurezza relativi ai prestatori di servizi fiduciari Servizi fiduciari qualificati Firme elettroniche Sigilli elettronici Validazione temporale elettronica Servizi elettronici di recapito certificato Autenticazione dei siti web	19 (dall'art. 20 al 24) (dall'art. 25 al 34) (dall'art. 35 al 40) (dall'art. 41 al 42) (dall'art. 43 al 44) 45
Documenti elettronici	Effetti giuridici dei documenti elettronici	46
Delega di potere e disposizioni di esecuzione (dall' art. 47 al 48)	Esercizio della delega conferito alla Commissione europea	47
Disposizioni finali (dall' art. 49 al 52)	Abrogazione Disposizioni transitorie Entrata in vigore	50 51 52

Identificazione elettronica

In tema di identificazione elettronica il Regolamento fornisce le seguenti definizioni:

Identificazione elettronica	Il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica
Mezzi di identificazione elettronica	Un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online
Dati di identificazione personale	Un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica
Regime di identificazione elettronica	Un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche
Autenticazione	Un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica

Il Regolamento si applicherà ai regimi di identificazione elettronica che saranno notificati dagli Stati membri e pertanto in Europa saranno riconosciuti e utilizzati almeno 28 differenti sistemi di "identificazione elettronica", differenti, uno per ogni Stato membro dell'Unione Europea. Ogni Stato membro potrà notificare all'Unione Europea il proprio sistema di identificazione elettronica ma tale regime notificato dovrà essere interoperabile.[48]

L'interoperabilità si realizza perseguendo i seguenti obiettivi:

a) si deve cercare di raggiungere la neutralità tecnologica e pertanto non sono ammesse discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro;

b) si deve essere "compliance", ove possibile, alle norme europee e internazionali;

c) si deve applicare il principio della privacy by design;

d) si devono garantire che i dati personali siano trattati in base alla disciplina europea di tutela dei dati personali in vigore.

All'art. 9 del Regolamento si prevede che ogni Stato membro debba comunicare in sede di notifica le seguenti informazioni:

[48] È stata emanata la Decisione di Esecuzione (UE) 2015/1984 della Commissione europea del 3 novembre 2015 che definisce le circostanze, i formati e le procedure della notifica regimi di identificazione elettronica.

a) una descrizione del regime di identificazione elettronica, con indicazione dei suoi livelli di garanzia e della o delle entità che rilasciano i mezzi di identificazione elettronica nell'ambito di tale regime;

b) il regime di vigilanza e il regime di informazioni sulla responsabilità applicabili per quanto riguarda:

- la parte che rilascia i mezzi di identificazione elettronica;
- la parte che gestisce la procedura di autenticazione;

c) l'autorità o le autorità responsabili del regime di identificazione elettronica;

d) informazioni sull'entità o sulle entità che gestiscono la registrazione dei dati unici di identificazione personale;

e) una descrizione di come sono soddisfatti i requisiti di interoperabilità;

f) una descrizione del sistema di autenticazione online da implementare per consentire alle parti facenti affidamento sulla certificazione stabilite nel territorio di un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica;

g) disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

Il Regolamento di esecuzione (UE) 2015/1501 della Commissione Europea dell'8 settembre 2015 ha stabilito i requisiti tecnici e operativi del quadro di interoperabilità al fine di garantire l'interoperabilità dei regimi di identificazione elettronica che gli Stati membri notificheranno all'Unione europea.

In tale contesto assume rilevanza il concetto di "nodo" definito come il punto di connessione facente parte di un'architettura di interoperabilità dell'identificazione elettronica, che interviene nell'autenticazione transfrontaliera delle persone ed è in grado di riconoscere ed elaborare le trasmissioni o di inoltrarle ad altri nodi attraverso l'abilitazione dell'interfacciamento dell'infrastruttura di identificazione elettronica nazionale di uno Stato membro con le infrastrutture di identificazione elettronica nazionale di altri Stati membri.

L'articolo 8 del Regolamento prevede che un regime di identificazione elettronica notificato debba specificare i livelli di garanzia (basso, significativo ed elevato) per i mezzi di identificazione elettronica rilasciati nell'ambito di tale regime medesimo.

Nella seguente tabella si riassumono i criteri alla base dei livelli di garanzia previsti nel Regolamento:

Livello di garanzia:	Dettagli:	Gestione del rischio:
Basso	Si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza limitato riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici.	Riduzione del rischio di uso abusivo o alterazione dell'identità.
Significativo	Si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza significativo riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici.	Riduzione significativa del rischio di uso abusivo o alterazione dell'identità.
Elevato	Si riferisce a un mezzo di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza più elevato dei mezzi di identificazione elettronica aventi un livello di garanzia significativo ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici.	Impedimento dell'uso abusivo o dell'alterazione dell'identità.

Il Regolamento di esecuzione (UE) 2015/1502 della Commissione Europea dell'8 settembre 2015, ha provveduto alla determinazione di specifiche, norme e procedure tecniche minime al fine di assicurare un'interpretazione comune dei dettagli dei livelli di garanzia e assicurare altresì l'interoperabilità nella mappatura dei livelli di garanzia nazionali dei regimi di identificazione elettronica notificati in base ai livelli di garanzia. Sono stati previsti un elenco di elementi necessari richiesti, in funzione del livello di garanzia, per una serie di fasi e sottofasi del processo di gestione dell'identificazione elettronica così definite:

Registrazione

– domanda di registrazione

– controllo e verifica dell'identità di una persona fisica;
– controllo e verifica dell'identità di una persona giuridica;
– collegamento tra i mezzi di identificazione elettronica delle persone fisiche e delle persone giuridiche

Gestione dei mezzi di identificazione elettronica

– caratteristiche e concezione dei mezzi di identificazione elettronica
– rilascio, consegna e attivazione
– sospensione, revoca e riattivazione
– rinnovo e sostituzione

Autenticazione

– Meccanismo di autenticazione

Gestione e organizzazione

– Disposizioni generali
– Pubblicazione di avvisi e informazioni per gli utenti
– Gestione della sicurezza delle informazioni
– Registrazione dei dati
– Strutture e personale
– Controlli tecnici
– Conformità e verifiche

A titolo esemplificativo, per la fase di registrazione e in riferimento al controllo e verifica dell'identità di una persona fisica si evidenziano nella tabella seguente gli elementi necessari in funzione del livello di garanzia previsti nel Regolamento di esecuzione (UE) 2015/1502:

Livello di garanzia:	Elementi necessari:
Basso	1. La persona può essere ritenuta in possesso di una prova riconosciuta dallo Stato membro in cui è presentata la domanda di rilascio del mezzo di identificazione elettronica e attestante l'identità dichiarata. 2. La prova può essere ritenuta autentica o esistente in virtù di una fonte autorevole[49] ed è all'apparenza valida. 3. L'esistenza dell'identità dichiarata è accertata mediante una fonte autorevole e si può presumere che la persona che sostiene di possederla sia la stessa e unica persona.

[49] Nell'allegato al Regolamento di esecuzione (UE) 2015/1502 con la locuzione "fonte autorevole" va intesa "qualsiasi fonte, a prescindere dalla forma, sulla quale si possa fare affidamento per l'ottenimento di dati, informazioni e/o elementi di prova esatti da utilizzare per dimostrare l'identità."

Livello di garanzia:	Elementi necessari:
Significativo	Livello basso, più una delle opzioni elencate di seguito ai punti da 1 a 4: 1. è stato verificato il possesso da parte della persona di una prova riconosciuta dallo Stato membro in cui è presentata la domanda di rilascio del mezzo di identificazione elettronica e attestante l'identità dichiarata e la prova è verificata per stabilirne l'autenticità oppure, secondo una fonte autorevole, esiste ed è collegata a una persona reale e sono state adottate misure per ridurre al minimo il rischio che l'identità della persona non corrisponda a quella dichiarata, tenendo conto ad esempio del rischio di smarrimento, furto, sospensione, revoca o scadenza della prova o 2. è presentato un documento d'identità durante un processo di registrazione nello Stato membro in cui è stato rilasciato il documento e quest'ultimo all'apparenza si riferisce alla persona che lo presenta e sono state adottate misure per ridurre al minimo il rischio che l'identità della persona non corrisponda a quella dichiarata, tenendo conto ad esempio del rischio di smarrimento, furto, sospensione, revoca o scadenza dei documenti o 3. ove procedure utilizzate in precedenza da un soggetto pubblico o privato nello stesso Stato membro per un fine diverso dal rilascio di mezzi di identificazione elettronica forniscano una garanzia equivalente a quelle definite in questa fase del processo (registrazione in riferimento al controllo e verifica dell'identità di una persona fisica) per il livello di garanzia significativo, l'entità responsabile della registrazione non è tenuta a ripeterle, purché detta garanzia equivalente sia confermata da un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008 del Parlamento europeo[50] e del Consiglio o da un organismo equivalente o 4. se i mezzi di identificazione elettronica sono rilasciati sulla base di un mezzo di identificazione elettronica notificato valido avente livello di garanzia significativo o elevato, e tenendo conto dei rischi di variazione dei dati di identificazione personale, non è necessario ripetere i processi di controllo e verifica dell'identità. Laddove il mezzo di identificazione elettronica che funge da base non sia stato notificato, il livello di garanzia significativo o elevato deve essere confermato da un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008 o da un organismo equivalente.

[50] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che disciplina la materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

Livello di garanzia:	Elementi necessari:
Elevato	Devono essere rispettati i requisiti di cui al punto 1 o 2. 1. Livello significativo, più una delle opzioni elencate di seguito alle lettere da a) a c): a) qualora sia stato verificato il possesso da parte della persona di una fotografia o di una prova di identificazione biometrica riconosciuta dallo Stato membro in cui è presentata la domanda di rilascio del mezzo di identificazione elettronica e qualora tale prova corrisponda all'identità dichiarata, la prova è verificata per stabilirne la validità in virtù di una fonte autorevole e il richiedente è identificato come corrispondente all'identità dichiarata tramite il confronto di una o più sue caratteristiche fisiche con una fonte autorevole o b) ove procedure utilizzate in precedenza da un soggetto pubblico o privato nello stesso Stato membro per un fine diverso dal rilascio di mezzi di identificazione elettronica forniscano una garanzia equivalente a quelle definite in questa fase del processo (registrazione in riferimento al controllo e verifica dell'identità di una persona fisica) per il livello di garanzia elevato, l'entità responsabile della registrazione non è tenuta a ripeterle, purché detta garanzia equivalente sia confermata da un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008 o da un organismo equivalente e sono intraprese azioni per dimostrare che i risultati delle procedure utilizzate in precedenza sono ancora validi o c) se i mezzi di identificazione elettronica sono rilasciati sulla base di un mezzo di identificazione elettronica notificato valido avente livello di garanzia elevato, e tenendo conto dei rischi di variazione dei dati di identificazione personale, non è necessario ripetere i processi di controllo e verifica dell'identità. Laddove il mezzo di identificazione elettronica che funge da base non sia stato notificato, il livello di garanzia elevato deve essere confermato da un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008 o da un organismo equivalente. e sono intraprese azioni per dimostrare che i risultati della precedente procedura di rilascio di un mezzo di identificazione elettronica notificato sono ancora validi. oppure 2. Qualora il richiedente non presenti una fotografia o una prova di identificazione biometrica riconosciuta, sono applicate le stesse procedure utilizzate a livello nazionale nello Stato membro dell'entità responsabile della registrazione per l'ottenimento di tale fotografia o prova di identificazione biometrica riconosciuta.

I Servizi fiduciari: quale perimetro

Fra le definizioni dell'art. 3 del Regolamento (punti 16 e 17) sono presenti quelle di servizio fiduciario e quelle di servizio fiduciario qualificato.

Per servizio fiduciario va inteso un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

– creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi;

oppure

– creazione, verifica e convalida di certificati di autenticazione di siti web;

oppure

– conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Il perimetro dei servizi fiduciari evidenziati nel Regolamento ed appena sopra esposti, non è però da considerarsi esaustivo e completo. Al punto 25 dei considerando del Regolamento viene infatti precisato che "È opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quali servizi fiduciari qualificati." Il Regolamento inoltre permette agli Stati membri di mantenere o introdurre disposizioni nazionali, conformemente al diritto dell'Unione, in materia di servizi fiduciari, nella misura in cui tali servizi non siano pienamente armonizzati dal Regolamento medesimo.

Tuttavia, i servizi fiduciari conformi al Regolamento devono godere della libera circolazione nel mercato interno.

Un servizio fiduciario che soddisfa i requisiti stabiliti nel Regolamento (in particolare le disposizioni dagli artt. 20 al 24) viene definito servizio fiduciario qualificato.

Firme elettroniche

Fra i servizi fiduciari più significativi, presidiati specificamente dal Regolamento, vi sono quelli di creazione, verifica e convalida di firme elettroniche. Nel Regolamento viene mantenuta la disciplina di tre differenti categorie di firme: la firma elettronica, la firma avanzata, la firma qualificata.

Le definizioni di firma avanzata e qualificata presenti nel Regolamento sono sostanzialmente allineate a quelle presenti nel CAD mentre la definizione di firma elettronica presenta differenze.

Nel Regolamento si definisce firma elettronica un insieme di "dati in

forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e *utilizzati dal firmatario per firmare*".[51]

Nel CAD si definisce firma elettronica "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, *utilizzati come metodo di identificazione informatica*."[52]

Il Regolamento non definisce né disciplina specificamente la firma digitale che rimane una particolarità dell'ordinamento italiano ed è definita nel CAD come "un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici."[53]

In un ambito di neutralità tecnologica, il Regolamento prevede che una firma elettronica avanzata deve soddisfare i seguenti requisiti:[54]

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Una delle novità più significative del Regolamento è la disciplina dei requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata:[55]

"1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:

a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;

b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;

---

(51) Art. 3 punto 10 del Regolamento.

(52) Art. 1 punto q del D.Lgs. 7 marzo 2005, n. 82 e successive modifiche.

(53) Art. 1 punto s del D.Lgs. 7 marzo 2005, n. 82 e successive modifiche.

(54) Art. 26 del Regolamento.

(55) Allegato II del Regolamento.

c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;

d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.

3. La generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciari qualificato."

La Commissione europea, con la Decisione di esecuzione (UE) 2015/1506, dell'8 settembre 2015, ha stabilito le specifiche relative ai formati delle firme elettroniche avanzate che gli organismi del settore pubblico devono riconoscere quando richiedono tali firme.

Le specifiche tecniche riportate nella tabella a seguire[56] riguardano i seguenti profili di firma:

– XAdES generalmente utilizzata per dati in formato XML;
– CAdES (cosiddetta P7M) per dati in qualsiasi formato;
– PAdES per dati in formato PDF.
– contenitore con firma associata per dati strutturati in contenitori come i file ZIP.

Elenco delle specifiche tecniche per le firme elettroniche avanzate XML, CMS o PDF e per il contenitore con firma associata

Le firme elettroniche avanzate di cui all'articolo 1 della decisione devono rispettare una delle seguenti specifiche tecniche ETSI, ad eccezione della clausola 9:

Profilo di base XAdES	ETSI TS 103171 v.2.1.1. (1)
Profilo di base CAdES	ETSI TS 103173 v.2.2.1. (2)
Profilo di base PAdES	ETSI TS 103172 v.2.2.2. (3)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
(2) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
(3) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Il contenitore con firma associata di cui all'articolo 1 della decisione deve rispettare le seguenti specifiche tecniche ETSI:

Profilo di base del contenitore con firma associata	ETSI TS 103174 v.2.2.1. (1)

(1) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

[56] Allegato alla Decisione di esecuzione (UE) 2015/1506, dell'8 settembre 2015.

Il Regolamento disciplina oltre agli effetti giuridici del documento elettronico, anche quelli delle firme elettroniche prevedendo che[57]:

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Nel CAD gli effetti giuridici del documento informatico sottoscritto con firma elettronica (in particolare l'efficacia probatoria), disciplinati dall'art. 21 sono riassunti nella tabella seguente:

Tipologia di firma	Efficacia probatoria
Firma elettronica semplice	Consente di ricondurre, in qualsiasi forma, dei dati elettronici ad un soggetto, ma non assicura l'integrità del documento stesso. Sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
Firma elettronica avanzata	Ha l'efficacia prevista dall'articolo 2702 del codice civile.[58] Soddisfa il requisito della forma scritta.[59]
Firma elettronica qualificata	Ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria Soddisfa il requisito della forma scritta.
Firma digitale	Ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria Soddisfa il requisito della forma scritta.

[57] Art. 25 del Regolamento.

[58] Art. 2702 del Codice civile - Efficacia della scrittura privata: "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta."

[59] Con il D.L. n. 179/2012 all'articolo 21, comma 2-*bis* del CAD è stato aggiunto il seguente periodo: "Gli atti di cui all'articolo 1350, primo comma, numero 13, del Codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale".

Il sigillo elettronico

Una delle novità più significative presenti nel Regolamento riguarda l'introduzione della disciplina del sigillo elettronico. Per sigillo elettronico s'intende un insieme di "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi".[60]

Il sigillo elettronico viene creato da una persona giuridica.[61]

Per creare un sigillo elettronico si possono utilizzare sia dispositivi software sia hardware opportunamente configurati.

Nel regolamento sono disciplinati tre differenti categorie di sigilli: i sigilli elettronici, i sigilli elettronici avanzati, i sigilli elettronici qualificati.

In un ambito di neutralità tecnologica, il Regolamento prevede che un sigillo elettronico avanzato deve soddisfare i seguenti requisiti:[62]

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

I requisiti relativi ai dispositivi per la creazione di un sigillo elettronico qualificato sono i medesimi previsti per la firma elettronica qualificata:[63]

Il Regolamento disciplina gli effetti giuridici del sigillo elettronico prevedendo che[64]:

a) è connesso unicamente al creatore del sigillo;

---

(60) Art. 3 del Regolamento.

(61) Nel considerando (68) del Regolamento si precisa quanto segue: "La nozione di «persone giuridiche» secondo le disposizioni del trattato sul funzionamento dell'Unione europea (TFUE) in materia di stabilimento lascia agli operatori la libertà di scegliere la forma giuridica che ritengono opportuna per svolgere la loro attività. Di conseguenza, per «persone giuridiche» ai sensi del TFUE si intendono tutte le entità costituite conformemente al diritto di uno Stato membro o da esso disciplinate, a prescindere dalla loro forma giuridica."

(62) Art. 3 del Regolamento.

(63) Allegato II del Regolamento.

(64) Art. 35 del Regolamento.

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

In tema di sigillo elettronico nei considerando del Regolamento si precisa quanto segue:

– (58) Qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.

– (59) È opportuno che i sigilli elettronici fungano da prova dell'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso.

– (60) I prestatori di servizi fiduciari che rilasciano certificati qualificati di sigilli elettronici dovrebbero attuare le misure necessarie per poter stabilire l'identità della persona giuridica rappresentante la persona fisica cui è fornito il certificato qualificato di sigillo elettronico, quando tale identificazione è necessaria a livello nazionale nel contesto di procedimenti giudiziari o amministrativi.

– (65) Oltre ad autenticare il documento rilasciato dalla persona giuridica, i sigilli elettronici possono anche servire ad autenticare qualsiasi bene digitale della persona giuridica stessa, quali codici di software o server.

La Commissione europea, con la Decisione di esecuzione (UE) 2015/1506, dell'8 settembre 2015, ha stabilito le specifiche relative ai formati dei sigilli elettronici avanzati che gli organismi del settore pubblico devono riconoscere quando richiedono tali firme. Nella tabella a seguire sono elencate tali specifiche.[65]

[65] Allegato alla Decisione di esecuzione (UE) 2015/1506, dell'8 settembre 2015.

Elenco delle specifiche tecniche per i sigilli elettronici avanzati XML, CMS o PDF e per il contenitore con sigillo associato

I sigilli elettronici avanzati di cui all'articolo 3 della decisione devono rispettare una delle seguenti specifiche tecniche ETSI, ad eccezione della clausola 9:

Profilo di base XAdES	ETSI TS 103171 v.2.1.1.
Profilo di base CAdES	ETSI TS 103173 v.2.2.1.
Profilo di base PAdES	ETSI TS 103172 v.2.2.2.

Il contenitore con sigillo associato di cui all'articolo 3 della decisione deve rispettare le seguenti specifiche tecniche ETSI:

Profilo di base del contenitore con sigillo associato	ETSI TS 103174 v.2.2.1.

Altri servizi fiduciari

Il Regolamento disciplina i seguenti ulteriori servizi fiduciari:
- Validazione temporale elettronica
- Validazione temporale elettronica qualificata
- Servizi elettronici di recapito certificato
- Servizi elettronici di recapito certificato qualificati
- Autenticazione dei siti web.

Con riferimento agli effetti giuridici della validazione temporale elettronica il Regolamento precisa che:[66]

1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.
2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.
3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.

Con riferimento agli effetti giuridici di un servizio elettronico di recapito certificato il Regolamento precisa che:

[66] Art. 41 del Regolamento.

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.
2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Al fine di diffondere fra i consumatori sicurezza e fiducia nelle transazioni commerciali on line, il legislatore europeo ha valutato opportuno introdurre anche una regolamentazione dei servizi di autenticazione dei siti web. Tali servizi dovrebbero permettere al visitatore di un sito di verificare che dietro a quel sito web vi sia un'entità effettiva e legittima. Anche se la fornitura e l'uso di servizi di autenticazione dei siti web rimane una scelta non obbligatoria per le imprese, il Regolamento disciplina gli obblighi minimi in materia di sicurezza e responsabilità per i prestatori e i loro servizi di autenticazione web.

Il Regolamento non vieta ai prestatori di servizi di autenticazione dei siti web di paesi extra Ue di prestare i propri servizi ai clienti dell'Unione. Tuttavia, i servizi di autenticazione dei siti web di un prestatore di un paese extra Ue devono essere riconosciuti come qualificati ai sensi del Regolamento solo se è stato concluso un accordo internazionale tra l'Unione e il paese di stabilimento di tale prestatore.

Effetti giuridici dei documenti elettronici

Il Regolamento persegue la neutralità sotto il profilo tecnologico. È considerato auspicabile che gli effetti giuridici prodotti dal Regolamento siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti.

In particolare il Regolamento conferma a livello unionale il principio di neutralità tecnologica rispetto alla forma elettronica di un documento.

L'art. 46 del Regolamento prevedendo che ad un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica, rafforza il principio di neutralità tecnologica.

I documenti elettronici sono considerati importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il Regolamento stabilendo il principio secondo cui a un documento elettronico non devono essere negati gli effetti giuridici per il motivo nella sua forma elettronica, mira ad assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica.

La valenza giuridica ed in particolare l'efficacia probatoria di un documento elettronico dipende dal livello di certezza dell'autenticità dell'origine e dell'integrità che il documento medesimo è in grado di assicurare durante l'intero suo ciclo di vita, dall'emissione fino al termine del periodo di sua conservazione, oltre naturalmente alla garanzia di disponibilità e leggibilità del documento medesimo.

Il Regolamento eIDAS e gli impatti sul Codice dell'Amministrazione digitale

Nell'ordinamento italiano non è presente una norma ad hoc che disciplina il collocamento dei regolamenti comunitari nel sistema delle fonti italiane di diritto.[67]

La Corte costituzionale ha preso nel tempo un orientamento sempre più filo-europeo. Secondo tale orientamento i regolamenti comunitari assumono una posizione equiparabile ad una legge nazionale con la specificità che in caso di conflitto con la legge nazionale, diventano prevalenti in quanto è stato affermato il principio del primato del regolamento sulle leggi ordinarie interne.

Il Regolamento e i suoi correlati atti di esecuzione, emanati e in corso di emanazione, disciplinando una serie di materie già presidiate dal Codice dell'Amministrazione Digitale (CAD)[68] e dalle Regole tecniche ad esso collegate, richiederà pertanto una serie di interventi, da parte del legislatore, per modificare ed integrare alcune delle disposizioni normative interne appena sopracitate, attualmente vigenti.

---

[67] La dottrina e la giurisprudenza ritengono che una collocazione dei regolamenti unionali possa essere determinata attraverso una lettura estensiva dell'art. 11 della Costituzione in cui si prevede che l'Italia "... consente, in condizioni di parità con gli altri Stati, alle limitazioni di sovranità necessarie ad un ordinamento che assicuri la pace e la giustizia fra le Nazioni."

[68] D.Lgs. 7 marzo 2005, n. 82 e successive modifiche.

L'art. 1 della legge n. 124 del 7 agosto 2015 (intitolata "Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche"), entrata in vigore il 28 agosto 2015, ha già delegato il Governo ad adottare, entro dodici mesi dalla data di entrata in vigore della legge appena sopracitata, uno o più decreti legislativi volti a modificare e integrare, anche disponendone la delegificazione, il CAD.

In particolare il comma 1 lettera p dell'articolo 1 della legge n. 124 del 7 agosto 2015 ha incaricato il Governo di adeguare l'ordinamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche e pertanto alle disposizioni previste nel Regolamento.

I punti principali di adeguamento del CAD dovrebbero riguardare almeno:

– un'armonizzazione delle definizioni;
– un ampliamento delle tipologie delle sottoscrizioni informatiche e dei certificati qualificati (firma elettronica, sigillo elettronico e autenticazione web);
– un aggiornamento delle regole di accreditamento per disciplinare i prestatori di servizi fiduciari qualificati;
– un aggiornamento di alcune regole tecniche esistenti quali il DPCM 22 febbraio 2013 in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

Lo schema delle modifiche del CAD riguardanti le materie di impatto sul mercato interno unionale dovrà essere notificato alla Commissione Europea.

Il Regolamento eIDAS e lo SPID

Al punto 13 dei considerando del Regolamento si afferma che: "è opportuno che gli Stati membri rimangano liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, e che possano decidere dell'eventuale partecipazione del settore privato nell'offerta di tali mezzi. È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione.

Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici."

Il comma 2 bis dell'art. 64 del D.Lgs. n. 82/2005 (CAD) prevede che, "per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese» (SPID)". Veniva demandato a un apposito decreto del Presidente del Consiglio dei ministri, la definizione delle caratteristiche del sistema SPID, nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle modalità attraverso cui le imprese possono avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti.

Lo SPID è pertanto il Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD.

Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

Con l'istituzione del sistema SPID, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi non solo mediante carta d'identità elettronica e la carta nazionale dei servizi ma anche mediante servizi offerti dal medesimo sistema SPID.

In sintesi lo SPID è un sistema di credenziali informatiche uniche ed interoperabili che dovrebbe consentire agli utenti di accedere a tutti i siti e servizi offerti dalla PA italiana. Al sistema SPID possono inoltre aderire inoltre servizi commerciali in Italia ed nell'Unione Europea che potranno così superare la criticità di dover registrare ex novo ed in maniera sicura e certa i propri clienti, utilizzando a tal fine lo SPID medesimo.

Il Decreto del Presidente del consiglio dei Ministri del 24 ottobre 2014 ha dato attuazione a quanto previsto all'art. 64 del CAD, disciplinando le caratteristiche del sistema SPID ed in particolare con riferimento:

– al modello architetturale e organizzativo del sistema;
– alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;
– agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire
– all'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese;

– alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

– ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

– alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

Il Governo italiano ha notificato alla Commissione europea il Decreto del Presidente del consiglio dei Ministri del 24 ottobre 2014 disciplinante lo SPID. Pertanto lo SPID dovrebbe diventare un regime di identificazione riconosciuto e accettato anche dagli altri Stati membri. Inoltre lo SPID si basa sulle specifiche OASIS SAML v2.0 diffuse a livello unionale ed adottate nel progetto sperimentale europeo Stork che ha come obiettivo primario lo sviluppo di un infrastruttura comune per l'identità digitale.[69]

[69] Per approfondimenti sul progetto Stork si veda: https://www.eid-stork.eu/

NUMERI PUBBLICATI

Anno 2007

- **nr. 1** L'amministrazione nelle S.r.l. • *Simone Allodi*
- **nr. 2** Lo Statuto dei diritti del contribuente • *Alessandro Turchi*
- **nr. 3** Finanziamento dei Soci • *Giorgio Zanetti*
- **nr. 4** Le norme del codice di procedura civile applicabili al Processo Tributario • *Paolo Brecciaroli*
- **nr. 5** Bilancio e misurazione della performance delle organizzazioni non profit: principi e strumenti • *Marco Grumo*
- **nr. 6** La normativa Antiriciclaggio. Profili normativi, obblighi ed adempimenti a carico dei dottori commercialisti • *Gian Gaetano Bellavia*
- **nr. 7** Limiti dell'informativa societaria e controllo dei bilanci infrannuali • *Roberta Provasi, Daniele Bernardi, Claudio Sottoriva*
- **nr. 8** La previdenza nella professione di Dottore Commercialista • *Ernersto Franco Carella*
- **nr. 9** L'introduzione dei Principi contabili internazionali e il coordinamento con le norme fiscali • *Mario Difino*
- **nr. 10** La governance delle società a partecipazione pubblica e il processo di esternalizzaziona dei servizi pubblici locali • *Ciro D'Aries*
- **nr. 11** Il Consolidato fiscale nazionale (artt. 117-129 TUIR e DM 9 giugno 2004) • *Ambrogio Picolli*
- **nr. 12** Il bilancio sociale nelle piccole e medie imprese • a cura di *Adriano Propersi*
- **nr. 13** Le parti e la loro assistenza in giudizio • *Mariacarla Giorgetti*

Anno 2008

- **nr. 14** Il nuovo ordinamento professionale: guida alla lettura del D.Lgs. n. 139 del 28 giugno 2005 • a cura della Commissione *Albo, Tutela e Ordinamento a 2005-2007*
- **nr. 15** Carta Europea dei diritti del contribuente • a cura della Commissione *Normative Comunitarie 2005-2007*
- **nr. 16** Elementi di procedura civile applicati alle impugnazioni del processo tributario • *Mariacarla Giorgetti*
- **nr. 17** Il processo di quotazione delle PMI tra presente e futuro: il ruolo del dottore commercialista in questa fase di cambiamento • *Carlo Arlotta*

- **nr. 18** Controlled Foreign Companies Legislation: Analisi comparata negli stati comunitari • *Sebastiano Garufi*
- **nr. 19** Il codice di condotta EU: Finalità e analisi comparativa a livello europeo • *Paola Sesana*
- **nr. 20** Il dottore commercialista e la pianificazione e il controllo nella PMI • *Aldo Camagni, Riccardo Coda, Riccardo Sclavi*
- **nr. 21** La nuova relazione di controllo contabile (art. 2409 ter del Codice Civile) • *Daniele Bernardi, Gaspare Insaudo, Maria Luisa Mesiano*

Anno 2009

- **nr. 22** L'azionariato dei dipendenti come forma di incentivazione: ascesa e declino delle stock option? • *Vito Marraffa*
- **nr. 23** Norme ed orientamenti rilevanti della Revisione Contabile • *Maria Luisa Mesiano, Mario Tamborini*
- **nr. 24** Gli accordi giudiziali nella crisi d'impresa • *Cesare Zafarana*, *Mariacarla Giorgetti, Aldo Stesuri*
- **nr. 25** Il bilancio consolidato e le scritture di consolidamento • *Francesco Grasso*, *Paolo Terazzi*
- **nr. 26** Conciliazione e mediazione: attualità legislative e profili operativi • *Aldo Stesuri*

Anno 2010

- **nr. 27** La crisi d'impresa - L'attestazione di ragionevolezza dei piani di ristrutturazione *ex* art. 67, 3° comma, lettera d) L.F. • *Commissione Gestione Crisi d'Impresa e Procedure Concorsuali*
- **nr. 28** Il Consolidato fiscale nazionale (artt. 117-129 TUIR e DM 9 giugno 2004) seconda edizione • *Ambrogio Picolli*
- **nr. 29** L'arbitrato - Analisi e commenti dalla recente prassi • *Commissione Arbitrato - a cura di Alessandro Augusto*
- **nr. 30** Il bilancio di sostenibilità delle multiutilities: esperienze a confronto • *Commissione Bilancio Sociale - a cura di Francesco Randazzo, Cristiana Schena, Gabriele Badalotti, Eros A. Tavernar*
- **nr. 31** La riforma della revisione legale in Italia: una prima analisi del D.Lgs. 39 del 27 gennaio 2010 • *Commissione Controllo Societario - Gruppo di lavoro: Daniele Bernardi, Antonella Bisestile, Alessandro Carturani, Annamaria Casasco, Gaspare Insaudo, Luca Mariani, Giorgio Morettini, Marco Moroni, Gianluca Officio, Massimiliano Pergami, Roberta Provasi, Marco Rescigno, Claudio Sottoriva, Mario Tamborini*
- **nr. 32** Obbligo P.E.C. - Opportunità e problematiche per gli studi professionali • *Commissione Informatica e C.C.I.A.A. - Gruppo di lavoro: Fabrizio Baudo, Davide Campolunghi, Filippo Caravati, Alberto De Giorgi, Gianluca De Vecchi, Pietro Longhi, Daniele Tumietto*
- **nr. 33** Nuova tariffa professionale - Commento alle modifiche intervenute • *Mario Tracanella*

Anno 2011

- **nr. 34** Perdite di valore e avviamento secondo i principi IFRS • *Riccardo Bauer, Claudia Mezzabotta*
- **nr. 35** Patrimonializzare e sostenere la competitività delle PMI italiane: la quotazione su AIM Italia • *Commissione Finanza e Controllo di Gestione - Gruppo di lavoro: Carlo Arlotta, Franco Bertoletti, Elisabetta Coda Negozio, Carlo Pesaro, Giorgio Venturini*
- **nr. 36** La mediazione civile – Novità normative e contesto operativo • *Gruppo di studio Commissione Mediazione e Conciliazione - a cura di Maria Rita Astorina e Claudia Mezzabotta*
- **nr. 37** La mediazione civile – Le tecniche di gestione dei conflitti • *Gruppo di studio Commissione Mediazione e Conciliazione - a cura di Maria Rita Astorina e Claudia Mezzabotta*
- **nr. 38** Caratteri e disciplina del concordato fallimentare • *Carlo Bianco, Mariacarla Giorgetti, Patrizia Riva, Aldo Stesuri, Cesare Zafarana*
- **nr. 39** Remunerare gli amministratori - Compensi incentivi e governance • *Gianluigi Boffelli*

Anno 2012

- **nr. 40** Scritti di Luigi Martino • *Comitato Editoriale - a cura di Gianbattista Stoppani e Dario Velo*
- **nr. 41** Aspetti fiscali delle operazioni straordinarie per i soggetti IAS/IFRS • *Commissione Diritto Tributario Nazionale - a cura di Emanuela Fusa*
- **nr. 42** L'accertamento tecnico dell'usura per le aperture di credito in conto corrente • *Commissione Banche, Intermediari Finanziari e Assicurazioni - a cura di Marco Capra, Roberto Capra*
- **nr. 43** Il nuovo concordato preventivo a seguito della riforma • *Commissione Gestione Crisi di Impresa e Procedure Concorsuali*
- **nr. 44** Introduzione all'Istituto del Trust • *Commissione Normative a Tutela dei Patrimoni*
- **nr. 45** Ambiti di applicazione del Trust • *Commissione Normative a Tutela dei Patrimoni*

Anno 2013

- **nr. 46** Arbitro Bancario Finanziario • *Commissione Metodi ADR*
- **nr. 47** Il rischio di continuità aziendale nel bilancio IAS ed in quello OIC • *Commissione Principi Contabili - a cura di Girolamo Matranga*
- **nr. 48** La mediazione civile nelle liti fra soci: profili giuridici ed efficacia negoziale • *Commissione Metodi ADR - a cura di Maria Rita Astorina, Marcella Caradonna*
- **nr. 49** La fiscalità della produzione nelle fonti di energie rinnovabili • *Commissione Diritto Tributario Nazionale - a cura di Federica Fiorani*
- **nr. 50** Il modello GBS 2013: lo standard italiano per la redazione del Bilancio Sociale • *Commissione Bilancio Integrato - a cura di Claudio Badalotti, Dario Velo, Gabriele Badalotti*

Anno 2014

- **nr. 51** I regolamenti appicativi del D.Lgs. 39/2010 sulla revisione legale dei conti emanati dal MEF • *Commissione Controllo Societario*
- **nr. 52** La previdenza nella professione di Dottore Commercialista • *Commissione Cassa Previdenza Dottori Commercialisti - a cura di Ernesto Carella*
- **nr. 53** Comunicare con Investitori e Finanziatori: il ruolo del Business Plan • *Commissione Finanza e Controllo di Gestione - a cura di Francesco Aldo De Luca e Alessandra Tami*
- **nr. 54** La Direttiva 2013/34/UE relativa ai bilanci d'esercizio e consolidati. – Novità e riflessi sulla disciplina nazionale • *Commissione Principi Contabili - a cura di Tiziano Sesana*
- **nr. 55** Gli obblighi di sicurezza nei luoghi di lavoro • *Commissione Lavoro - a cura di Monica Bernardi, Bernardina Calafiori, Gabriele Moscone, Patrizia Rossella Sterza, Sergio Vianello*
- **nr. 56** Le Start-up innovative • *Commissioni Start-up, Microimprese e Settori Innovativi e Diritto Tributario Nazionale - a cura di Antonio Binacchi e Alessandro Galli*

Anno 2015

- **nr. 57** Il Concordato preventivo: riflessioni teoriche • *Commissione Gestione Crisi di Impresa e Procedure Concorsuali - a cura di Giannicola Rocca*
- **nr. 58** Il Concordato preventivo: esperienze empiriche • *Commissione Gestione Crisi di Impresa e Procedure Concorsuali - a cura di Giannicola Rocca*
- **nr. 59** Il controllo della liquidità nelle strategie aziendali e nelle situazioni di crisi. Il contributo del business plan • *Commissione Finanza e Controllo di Gestione - a cura di Carlo Arlotta, Salvatore Carbone, Francesco Aldo De Luca, Alessandra Tami*
- **nr. 60** La collaborazione volontaria. Idiversi perchè di una scelta (quasi) obbligata • *Commissione Normative a Tutela dei Patrimoni - a cura di Marco Salvatore, Paolo Ludovici, Fabrizio Vedana*
- **nr. 61** Relazione di revisione. Le novità al giudizio sul bilancio introdotte dagli ISA Italia • *Commissione Controllo Societario - a cura di Daniele Bernardi, Gaspare Insaudo, Luca Magnano San Lio, Claudio Mariani*
- **nr. 62** Accertamento sintetico, redditometro e "redditest" • *Commissione Diritto Tributario Nazionale - a cura di Alessandro Cerati*

Anno 2016

- **nr. 63** Il Consolidato fiscale nazionale (artt. 117-129 TUIR e DM 9 giugno 2004) • terza edizione • *Commissione Diritto Tributario Nazionale - a cura di Ambrogio Andrea Picolli*
- **nr. 64** Revisione della contabilità di condominio • *Gruppo di lavoro della Commissione Amministrazioni Immobiliari*
- **nr. 65** Appunti per una cultura di parità • *Commissione Pari Opportunità - a cura di Grazia Ticozzelli*

finito di stampare
nel mese di settembre 2016

3LB srl
Osnago (LC)

nr. 66.

La “dematerializzazione documentale” (gestione su supporto elettronico di documenti a rilevanza giuridica) è tema pervasivo per la Professione. Si tratta di adempiere a precisi obblighi di legge e di approfondire il fenomeno e gli scenari sottesi per saperne cogliere le opportunità per lo Studio e la Clientela.
La materia, trasversale, ha peraltro conosciuto una espansione esponenziale, generando ulteriori specializzazioni. Per questo, si è evitato un approccio “omnicomprensivo”, preferendo operare una scelta ragionata di temi, comunque sistematicamente collegati, ritenuti di maggior momento per il Professionista, in particolare nel suo ruolo di consulente giuridico e organizzativo. La trattazione ha pertanto carattere sia teorico, sia immediatamente applicativo e, per quanto selettiva, ha avuto necessità di un respiro conforme alle esigenze professionali.
I temi trattati sono stati quindi raccolti in due Quaderni, costituenti Parti di un’opera comunque unitaria: la prima, se vogliamo, di carattere più generale e trasversale, la seconda focalizzata sul tema, forse di maggior attualità e notorietà, della fattura elettronica.

Pietro Luca Agostini, Dottore Commercialista, Revisore Legale, Commissione Informatica CCIAA Registro Imprese Milano ODCEC Milano.

Ruggiero Delvecchio, Dottore Commercialista, Revisore Legale, Commissione Informatica CCIAA Registro Imprese Milano ODCEC Milano.

Davide Grassano, Dottore Commercialista, Revisore Legale, Commissione Informatica CCIAA Registro Imprese Milano ODCEC Milano.

Giuseppe Mantese, Dottore Commercialista, Revisore Legale, Commissione Informatica CCIAA Registro Imprese Milano ODCEC Milano.

Francesco Milano, Dottore Commercialista, Revisore Legale, Commissione Informatica CCIAA Registro Imprese Milano ODCEC Milano.

ISSN 1971-2456