Rivista elettronica di Diritto, Economia, Management

Numero 4 - 2024

Il regolamento eIDAS n. 2024/1183.

Numero speciale curato dall'ing. Giovanni Manca.

Prefazione del Senatore Alessio Butti, Sottosegretario di Stato con delega all'innovazione tecnologica.

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

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOeDU®

ISSN 2039-4926

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente, che ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla trasformazione digitale, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo nei settori pubblico e privato.
La rivista ha anche la finalità di ospitare contributi di giovani studiosi per valorizzarne le attitudini alla ricerca e il loro contributo allo sviluppo delle scienze giuridiche, sociali, economiche e manageriali.

Direttore responsabile: Donato A. Limone

Comitato scientifico: Estanislao Arana García, Catedrático de Derecho administrativo de la Universidad de Granada (Spagna); Raffaele Barberio (Esperto in mercati digitali e presidente di Barberio&Partners); Piero Bergamini (Comitato Direttivo del Club degli Investitori di Torino); Francesco Capriglione (professore di diritto degli intermediari e dei mercati finanziari, Luiss, Roma); Enzo Chilelli (esperto di sanità e di informatica pubblica); Claudio Clemente (Banca d'Italia); Fabrizio D'Ascenzo (già Preside della Facoltà di Economia, Università Sapienza; presidente INAIL); Sandro Di Minco (avvocato, ha insegnato informatica giuridica nelle università di Camerino, Chieti-Pescara, Macerata, Sapienza, Teramo); Luigi Di Viggiano (Università del Salento; esperto di scienza dell'amministrazione digitale); Jorge Eduardo Douglas Price, ordinario di Teoria generale del diritto; Direttore del Centro di Studi Istituzionali Patagónico (CEIP), Facoltà di Giurisprudenza e Scienze Sociali dell'Università Nazionale di Comahue (Argentina); Massimo Farina, abilitato alle funzioni di professore ordinario per SSD IUS/20, Università di Cagliari; Maria Rita Fiasco (consulente, Vice Presidente Assinform); Antonella Galdi (Vice Segretario Generale ANCI); Donato A. Limone (già ordinario di informatica giuridica; fondatore e direttore della "Rivista elettronica di diritto, economia, management"); Andrea Lisi (Avvocato, docente ed esperto di Diritto dell'Informatica; Presidente di Anorc Professioni); Valerio Maio (ordinario di diritto del lavoro, Università degli Studi di Roma, Unitelma Sapienza); Marco Mancarella (professore associato di informatica giuridica, Unisalento); Gianni Penzo Doria (professore associato di archivistica e di diplomatica, Università degli Studi dell'Insubria); Nadezhda Nicolaevna Pokrovskaia (docente universitario presso Herzen State Pedagogical University of Russia e Peter the Great Saint-Petersburg Polytechnic University); Ranieri Razzante (Docente di Tecniche e regole della cybersecurity nell'Università Suor Orsola Benincasa, Napoli) ; Francesco Riccobono (ordinario di teoria generale del diritto, Università Federico II, Napoli); Andrea Sacco Ginevri (ordinario di diritto dell'economia, Università Roma 3); Fabio Saponaro (professore ordinario di diritto tributario, Università del Salento); Marco Sepe (ordinario di diritto dell'economia, Università degli studi di Roma, Unitelma Sapienza).

Comitato di redazione: Alberto Bruni, Angelo Cappelli, Luca Caputo, Claudia Ciampi, Ersilia Crobe, Tiziana Croce, Paola Di Salvatore, Santo Gaetano, Paolo Galdieri, Salvatore Gallo, Fabio Garzia, Edoardo Limone, Emanuele Limone, Lorenzo Locci, Lucio Lussi, Antonio Marrone, Alessio Mauro, Daniele Napoleone, Alberto Naticchioni, Cristina Evanghelia Papadimitriu, Giulio Pascali, Gianpasquale Preite, Sara Sergio, Franco Sciarretta.

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

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

Anno XIV, n. 4/2024
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

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

Codice etico: *www.clioedu.it/rivistaelettronica#codice-etico*
Procedure di referaggio: *www.clioedu.it/rivistaelettronica#referaggio*
Elenco dei numeri pubblicati: *www.clioedu.it/rivistaelettronica*

Indice

Editoriale
Donato A. Limone 4

Prefazione
Alessio Butti, Senatore e Sottosegretario di Stato
con delega all'innovazione tecnologica 6

Introduzione
Giovanni Manca, curatore del numero 9

Il nuovo regolamento eIDAS tra identità digitale europea e firme elettroniche
Andrea Valle 11

Il regolamento eIDAS n. 2024/1183 ed il Codice dell'amministrazione digitale.
Alcune considerazioni su modifiche ed integrazioni
Donato A. Limone 20

Il regolamento eIDAS 2.0 e l'impatto sulla gestione documentale delle PA:
quali prospettive?
Ernesto Belisario 32

L'evoluzione del documento informatico nel nuovo quadro giuridico dell'eIDAS 2
Andrea Lisi 42

European Digital Identity Wallet, nuova era del decennio digitale
Beatrice Tafini 54

La protezione dei dati personali nell'architettura del portafoglio europeo
Sarah Ungaro 62

Il ruolo degli standard in eIDAS 2.0
Andrea Caccia 71

European Digital Identity Wallet: impatti su protezione dei dati personali e sicurezza
Marco Mangiulli 81

L'interoperabilità del portafoglio d'identità europeo
Andrea De Maria 88

eIDAS 2.0: la sostenibilità come leva per una rapida diffusione
Andrea Sassetti 93

L'attestazione elettronica di attributi
Giovanni Manca 100

L'avvento dei QWAC: una svolta epocale nella governance dei certificati SSL
Adriano Santoni 105

Dalla conservazione all'e-archiving. I requisiti che un qualified trust service provider deve possedere per erogare il servizio di e-archiving: prospettive e scenari per il mercato
Patrizia Sormani 126

Le potenzialità di eIDAS 2.0 sui servizi di conservazione digitale: stato dell'arte, impatti tecnologici e prospettive
Enrico Giunta – Federica Marti 145

Registri elettronici qualificati: tecnologie ed opportunità
Davide Colletto – Giulio Di Clemente 164

Il nuovo sistema sanzionatorio in eIDAS 2.0: ruolo di AgID e questioni applicative
Massimiliano Nicotra 176

Firme elettroniche avanzate: nuovi riferimenti e vecchi problemi irrisolti
Luigi Foglia 186

Le nuove regole europee per la sottoscrizione e l'apposizione di sigilli in modalità remota
Giovanni Manca 196

Regolamento eIDAS 2.0 e firma elettronica qualificata: nuovi scenari e opportunità
Simone Baldini 201

Le procedure di identificazione del titolare nel Regolamento 2024/1183 (eIDAS 2): prospettive europee e nazionali
Igor Marcolongo 208

Il recapito elettronico: scenari ed evoluzione tecnologica alla luce degli aggiornamenti normativi in Italia e in Europa
Flavio Fanton – Enrico Giunta – Federica Marti 223

La firma elettronica qualificata gratuita nel portafoglio europeo di identità digitale
Giovanni Manca 235

Autori di questo numero 241

N. 4 - 2024 - pp. 4-5

Editoriale

Questo numero della Rivista è dedicato al regolamento UE 2024/1183 che modifica il regolamento UE 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a *un'identità digitale* (eIDAS - electronic Identification Authentication and Signature) e al *portafoglio digitale* dei servizi basato appunto sulla identità digitale unica, sicura e interoperabile. L'incidenza di questo regolamento sui servizi digitali pubblici e privati, sia a livello europeo e sia a livello dei singoli Paesi membri della Unione, sarà molto forte e determinante per uno sviluppo del mercato interno dei servizi. In particolare, il regolamento determinerà la riduzione (sia pure graduale ma sensibile) al ricorso alla "certificazione pubblica" (analogica e/o digitale) per potere effettuare i servizi digitali in quanto tale certificazione (che comporta oggi un aggravio burocratico molto elevato e su tutti i settori) sarà "superata" dalla integrazione tra identità digitale e attributi personali. La prefazione del volume è di Alessio Butti, Senatore e Sottosegretario di Stato con delega all'innovazione tecnologica.

Il volume è curato da Giovanni Manca uno dei più importanti attori degli ultimi 30 anni in Italia sulla scena del digitale sotto il profilo della regolazione tecnica e non solo (rinvio al suo volume *Memorie del digitale. Cronache, storie e aneddoti della trasformazione digitale*, Edizioni Themis, 2024). *Questo numero della Rivista costituisce la prima analisi organica sul regolamento sotto il profilo giuridico e tecnico*. Di Giovanni Manca i contributi sull'attestazione elettronica di attributi, le nuove regole europee per la sottoscrizione e l'apposizione di sigilli in modalità remota, la firma elettronica qualificata gratuita nel portafoglio europeo di identità digitale. Contributi di carattere generale sono quelli di Andrea Valle (il nuovo regolamento eIDAS tra identità europea e firme elettroniche) e Donato Limone (eIDAS e il codice dell'amministrazione digitale). Due contributi specifici trattano del *documento informatico* (Andrea Lisi) e della *gestione documentale* (Ernesto Belisario). Sul *portafoglio digitale* gli articoli di Beatrice Tafini, Mauro Mangiulli, Andrea De Maria. Sulla *protezione dei dati personali* nell'architettura del portafoglio europeo rinvio al contributo di Sarah Ungaro. Andrea Caccia tratta il tema degli *standard* in eIDAS 2. Sulla *sostenibilità* come leva per una rapida diffusione del portafoglio l'articolo di Andrea Sassetti. Adriano Santoni interviene sull'avvento del QWAC (come svolta epocale della governance dei certificati SSL). Sui requisiti e sistemi di *conservazione e archiviazione* gli articoli di Patrizia Sormani e di Enrico Giunta-Federica Marti. Sui

registri elettronici qualificati lo scritto di Davide Colletto e Giulio Di Clemente. Sulle *firme elettroniche* rinviamo ai contributi di Luigi Foglia, Giovanni Manca, Simone Baldini. Lo scritto di Igor Marcolongo riguarda le procedure di *identificazione* del titolare del regolamento eIDAS2; sul *recapito elettronico* intervengono Flavio Fanton, Enrico Giunta, Federica Marti. Sul nuovo *sistema sanzionatorio* in eIDAS2 il contributo di Massimiliano Nicotra.

Ringrazio il curatore e gli autori di questo numero per questa prima analisi organica del regolamento eIDAS/2 con contributi scientifici e tecnici molto importanti.

Il Direttore della Rivista
Donato A. Limone

N. 4 - 2024 - pp. 6-8

Prefazione

Identità digitali e digital wallet: un traguardo importante per l'Italia e per l'Europa

Perchè è così importante tagliare il duplice traguardo di un'identità digitale europea e di un portafoglio digitale dei servizi ad essa associato? Delle molte possibili, credo sia questa la prima, e più importante, delle domande da porsi nell'affrontare la lettura dei numerosi (e ottimi) contributi che popolano questo numero monografico della Rivista elettronica di diritto, economia e management. Una domanda – aggiungo – niente affatto scontata, come peraltro dimostrano le risposte che raccoglie.

Tre di queste risposte sono particolarmente importanti. La prima è di ordine storico. Richiede quindi un breve viaggio a ritroso nel tempo. Un salto indietro di due decenni, per l'esattezza. Correva l'anno 2000, inizio simbolico di un nuovo decennio, di un nuovo secolo e di un nuovo millennio. Il mondo di allora, che un osservatore superficiale probabilmente giudicherebbe non così diverso da quello di oggi, era in realtà molto lontano dalla contemporaneità che viviamo. In ordine sparso e a giovamento dei nostalgici (ma non solo): nel 2000 la popolazione mondiale raggiungeva quota sei miliardi. Sono due miliardi di individui in meno rispetto a quelli che oggi popolano il pianeta. Iniziava la storia dell'Euro, che nel gennaio di quell'anno diventava ufficialmente valuta ufficiale di dodici Paesi, tra cui l'Italia. George W. Bush vinceva in modo rocambolesco le presidenziali negli Stati Uniti. Nel frattempo la bolla speculativa delle cosiddette "dot-com" raggiungeva il suo apice. Di li a breve avrebbe mietuto molte vittime, soprattutto tra piccoli e medi investitori che avevano creduto, e sperato, in guadagni che il senno di poi avrebbe rivelato evidentemente troppo facili.

Il 2000 è anche l'anno in cui entra in vigore negli Stati Uniti l'ESIGN Act, che attribuisce validità legale alla firma elettronica, aprendo la strada alla diffusione su larga scala delle firme elettroniche in ambito commerciale e legale. È a tutti gli effetti una rivoluzione nel modo di pensare e gestire le relazioni tra Stato, cittadini e imprese commerciali. Una rivoluzione iniziata qualche anno prima: nel novembre 1999 la Direttiva europea 93/1999 aveva definito un quadro unitario sulle firme elettroniche. Ancora prima, nel 1997, il nostro Paese aveva normato (primo al mondo) la validità giuridica del documento informatico e delle firme digitali.

Di certo c'è un fatto: la firma digitale è stata uno dei pilastri che ha permesso di realizzare il più grande blocco commerciale al mondo, il mercato unico europeo, facilitandone l'integrazione e il funzionamento. Se oggi questo mercato registra transazioni commerciali interne per un valore di 3,6 trilioni di Euro è anche grazie al riconoscimento di validità legale delle firme elettroniche. Ecco dunque una prima risposta alla nostra domanda. L'evoluzione delle norme europee in tema di firma digitale (eIDAS 2.0) rappresenta un passo avanti importantissimo verso un'Unione che vogliamo capace di crescere, competere e innovare ma, al tempo stesso, forte nel sostenere e promuovere i diritti individuali e collettivi.

La seconda risposta alla domanda iniziale è in continuità con la prima, ma capovolge la prospettiva: ci proietta verso il futuro. La nuova normativa eIDAS, che introduce un portafoglio di identità digitale europeo, sostanzialmente ci pone all'interno di un quadro di maggiori garanzie per la sicurezza, di migliore accessibilità digitale e di più elevata capacità di competere per il tessuto imprenditoriale europeo.

La sicurezza dei dati digitali è una condizione oramai imprescindibile per qualsivoglia politica pubblica che ambisca a regolare la frontiera tecnologica con lungimiranza ed efficacia. I dati, che un tempo celebravamo enfaticamente come il nuovo "petrolio", sono divenuti a tutti gli effetti la moneta di scambio e il collante di società ed economie ad alto tasso di digitalizzazione. A una condizione: che siano posti in sicurezza. Facile a dirsi, più complesso a farsi. Ancora nel 2023, solamente sei cittadini europei su dieci avevano la possibilità di utilizzare un'identità elettronica affidabile a livello transfrontaliero. Troppo pochi per un mercato unico di dimensioni così vaste e ambizioni (legittimamente) così elevate. Le nuove norme europee pongono finalmente le condizioni essenziali per migliorare la fiducia dei cittadini nei servizi digitali e promuovere un ambiente sicuro e trasparente.

Dalla sicurezza all'accessibilità: con il portafoglio di identità digitale i cittadini avranno la possibilità di accedere in modo ancora più semplice ai servizi pubblici e privati. Non dimentichiamo che quello della completa digitalizzazione delle interazioni tra individui e pubbliche amministrazioni è un obiettivo cardine del decennio digitale europeo che stiamo attraversando – e di riflesso del mandato governativo in tema di digitalizzazione. Superfluo dire che è anche questo un obiettivo ambizioso e sfidante, che però proprio grazie alle nuove norme acquisisce maggiore concretezza. Pensate alla possibilità di gestire digitalmente documenti come diplomi universitari, patenti di guida o biglietti del treno, tutti in un singolo spazio virtuale. È un vero e proprio salto quantico all'interno di quella dimensione umana semplificata che accompagna (e di fatto definisce) l'idea stessa di trasformazione digitale.

Non ultimo, il lato imprese. Le nuove norme europee semplificano i processi di autenticazione e riducono costi associati. Per un'azienda significa avere a disposizione un'arma in più per effettuare operazioni transfrontaliere e, al tempo stesso, migliorare la fiducia dei propri clienti. Da anni ormai portiamo avanti un dibattito che si interroga sulle ragioni di una minore competitività delle imprese europee rispetto a quelle extra-europee, soprattutto in alcuni settori, tra cui quello digitale.

Naturalmente la causa non è una sola, ma certamente include una serie di barriere burocratiche all'ingresso che hanno impedito ai nostri imprenditori di scalare più rapidamente. Rimuovere uno di quegli ostacoli è una formidabile iniezione di fiducia per le aziende e per i consumatori.

La terza risposta al quesito sull'importanza delle nuove norme europee è forse la più importante, oltre che quella che dovrebbe renderci più orgogliosi, da italiani. Il nostro Paese è infatti tra le teste di serie in Europa sia sul fronte delle identità digitali, sia per la realizzazione del *digital wallet*.

Quanto alle prime, il processo di razionalizzazione avviato dal governo Meloni ha permesso di superare l'eccezionalità di un sistema di identità digitali che soffriva dei disequilibri pubblico-privato e di avviare una transizione a un sistema pubblico più sicuro, più accessibile e a minor costo. Tradotto in parole semplici: non eliminiamo le identità digitali private, ma rafforziamo le identità digitali pubbliche. Ancora più importanti sono i traguardi raggiunti dal punto di vista del portafoglio digitale. La sperimentazione con l'IT-Wallet ha preso le mosse da documenti come la tessera sanitaria, ma arrivarà molto presto a includere tutti i principali documenti, a vantaggio dei nostri cittadini.

Il baricentro di tutti questi sforzi, frutto del lavoro congiunto tra Dipartimento per la Trasformazione Digitale, Ministeri, Agenzie nazionali e naturalmente di tutte le articolazioni amministrative sul territorio, è nella volontà di rendere l'esperienza utente soddisfacente, perchè sicura, semplice e abilitante. Un domani, non troppo lontano, l'identificazione digitale sarà il punto di accesso a sistemi predittivi capaci di anticipare e reagire ai bisogni del titolare in tempo reale. Oggi è la chiave attraverso cui realizzare uno Stato e un'Europa digitali vicini ai bisogni delle persone e delle imprese.

Alessio Butti
Senatore e Sottosegretario di Stato
con delega all'innovazione tecnologica

N. 4 - 2024 - pp. 9-10

Introduzione

Giovanni Manca

Il 20 maggio 2024 è entrato in vigore il regolamento (UE) 2024/1183 del Parlamento Europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

La protagonista assoluta, già nel titolo, è l'identità digitale che si stabilisce essere unica, sicura e interoperabile a livello dell'Unione.

L'attuazione di questi principi è demandata al Portafoglio Europeo di Identità Digitale, con titolarità di persone fisiche e giuridiche, che è mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro i propri dati di identità ma anche le attestazione degli attributi che caratterizzano l'identità stessa. Questi dati possono essere scambiati tra titolari e terza parti che ne fanno affidamento operativo. La possibilità per le persone fisiche di firmare gratuitamente (tramite il portafoglio) in modo equivalente alla firma autografa con la firma elettronica qualificata conferiscono ulteriore spessore allo scenario di applicazione di questo regolamento.

L'identità digitale è accompagnata da altre novità sui servizi fiduciari stabiliti nel regolamento 2024/1183. C'è la gestione di dispositivi per la creazione di una firma elettronica a distanza accompagnata dall'analoga gestione di dispositivi per la creazione di un sigillo elettronico a distanza. Questi servizi sono indispensabili per l'uso, associato al Portafoglio, per la sottoscrizione o l'apposizione di sigilli ai dati e ai documenti elettronici.

Questi poi possono essere archiviati o registrati con gli specifici servizi fiduciari, anch'essi introdotti dal regolamento qui indicato.

Gli autori che hanno contribuito con cortesia, competenza ed entusiasmo a questo numero della rivista trattano le varie tematiche descrivendo le varie novità sugli specifici servizi fiduciari e approfondiscono argomenti importanti come il trattamento dei dati personali, il nuovo regime sanzionatorio e anche le novità per i certificati di autenticazione dei siti web, già presenti nel regolamento 2014/910, ma con nuove regole in questa nuova versione normativa.

La lettura di questo numero della rivista consente di avere un quadro aggiornato sui temi dell'identità digitale europea e dei più importanti e innovativi servizi fiduciari ipotizzando anche nuovi scenari operativi per tutte le novità ad essi relative. Non manca un'analisi delle prospettive di mercato per l'identità digitale e i por-

tafogli, per questi ultimi anche in termini di sostenibilità economica.

La sfida nell'Unione è quella di una identità digitale attenta alla protezione dei dati personali tramite livelli di sicurezza allo stato dell'arte, a supporto di nuovi servizi in rete, sia pubblici che privati. Questa sfida deve prestare attenzione ai rischi di frammentazione del mercato che potrebbe mantenere localismi nei servizi digitali o avere un numero troppo elevato di istanze private dei portafogli. Il rischio di prevalenza dei colossi tecnologici anche in questi nuovi scenari deve essere gestito con attenzione, al fine di raggiungere l'unico vero obiettivo di tutte queste novità, la fiducia dei cittadini nei servizi digitali.

N. 4 - 2024 - pp. 11-19

Il nuovo Regolamento eIDAS tra identità digitale europea e firme elettroniche

Andrea Valle

Abstract [IT]: Lo scorso 30 aprile 2024 è stata pubblicato nella Gazzetta Ufficiale della Comunità Europea il regolamento 2024/1183, come revisione del Regolamento (UE) n. 910/2014 (meglio conosciuto come Regolamento eIDAS) che rappresenta il testo normativo di riferimento dell'Unione Europea nell'ambito di identità digitale, firme elettroniche e altri servizi fiduciari. Si tratta di una revisione profonda, dopo dieci anni che hanno visto la prima edizione portare significativi progressi nell'adozione di strumenti fondamentali per la trasformazione digitale come le firme elettroniche, ma accompagnati anche da risultati non altrettanto brillanti dal punto di vista dell'adozione in ambito "cross-border", ovvero nelle transazioni transfrontaliere che coinvolgono diversi paesi membri. La versione aggiornata del Regolamento eIDAS, spinta da un tessuto socioeconomico in continua trasformazione, introduce alcune novità importanti che puntano ad aumentare sia la tipologia che l'interoperabilità dei servizi fiduciari, favorendone l'adozione ad un numero più elevato di cittadini ed imprese.

Abstract [EN]: On 30 April 2024, regulation 2024/1183, was published in the Official Journal of the European Community, as revision of the regulation (EU) 910/2014 (better known as the eIDAS Regulation) which represents the reference regulatory text of the European Union in the field of digital identity, electronic signatures and other trust services. This is a review This is a major overhaul, after ten years from the first edition which made significant progress in the adoption of key tools for digital transformation such as electronic signatures, but also accompanied by less-than-stellar results from the point of view of adoption in the "cross-border" sphere, for transactions involving multiple member states. Driven by the evolving socio-economic fabric, the updated version of the eIDAS Regulation introduces some important innovations that aim to increase both the type and interoperability of trust services and to facilitate their adoption by a larger number of citizens and businesses.

Parole chiave: eIDAS, Identità elettronica, Firme elettroniche, Sigilli elettronici, Servizi fiduciari, Atti di esecuzione, Portafoglio Europeo di Identità Digitale, European Digital Identity Wallet, EDIW, Attributi elettronici, Certificati di autenticazione web, QWAC, Archiviazione elettronica, Registri elettronici.

Sommario: 1. Introduzione – 2. Il quadro europeo relativo all'identità digitale – 3. I portafogli europei di identità digitale – 4. Attestazione elettronica di attributi – 5. Firme elettroniche qualificate gratuite – 6. Certificati qualificati per l'autenticazione di siti Web – 7. Archiviazione elettronica qualificata – 8. Registri elettronici – 9. Conclusioni

1. Introduzione

Il 30 aprile 2024 è stato pubblicato sulla Gazzetta Ufficiale comunitaria il regolamento 2024/1183 che aggiorna il Regolamento UE n. 910/2014, noto anche come eIDAS (acronimo di "Electronic IDentification and trust Services"), pubblicato esattamente dieci anni fa ed entrato in vigore nel 2016. La revisione è stata stimolata dalla limitata implementazione da parte degli Stati membri dell'UE, soprattutto nell'ambito dell'identità digitale. Il nuovo Regolamento prevede di fornire strumenti affidabili e sicuri per l'utilizzo di identità digitali verificate con servizi accessibili non solo nell'ambito pubblico, ma anche in quello privato.

Nel giugno 2021 la Commissione Europea propose di modificare e aggiornare il Regolamento eIDAS rispondendo alle sfide sollevate dalle sue carenze strutturali e dalla limitata attuazione in alcuni suoi ambiti, nonché agli sviluppi tecnologici intervenuti dopo la sua adozione nel 2014. I risultati della valutazione della Commissione sull'impatto del Regolamento hanno fatto luce sulle varie limitazioni che gli hanno impedito di realizzare il suo pieno potenziale, evidenziando le insidie da superare e gli obiettivi mancati, stabilendo così il contesto per la sua revisione.

La proposta della Commissione si è focalizzata sullo sviluppo di un quadro europeo relativo all'identità digitale per fornire un modo affidabile e sicuro per autenticare e condividere online dati qualificati, attraverso un "portafoglio di identità digitale" garantito dagli Stati membri e che consenta transazioni in tutta l'UE. L'obiettivo da raggiungere fissato nel "Percorso verso il decennio digitale" dell'Europa, prevede che l'80% dei cittadini dell'Unione abbia accesso alla propria Identità Digitale entro il 2030, un obiettivo di crescita significativo dato il livello attuale di adozione pari al 59%, con solo 14 Stati membri che hanno notificato alla Commissione almeno un sistema pubblico di identità digitale.

Inoltre, la proposta di revisione dà seguito alla visione e alla richiesta esplicita del Consiglio europeo di realizzare l'identificazione elettronica pubblica e sicura (eID) a livello europeo, includendo firme digitali interoperabili, dando ai cittadini dell'Unione Europea il controllo della propria identità online e dei relativi dati, consentendo l'accesso a servizi digitali pubblici, privati e transfrontalieri.

In questo articolo vogliamo riassumere i punti essenziali che contraddistinguono questa attesa revisione del Regolamento eIDAS, focalizzandoci sugli elementi di novità che puntano a realizzare i maggiori benefici per i cittadini e le imprese. Altri articoli di questo numero della Rivista esamineranno alcune tematiche in maniera

più specifica e ad essi si rimanda il lettore per approfondirle.

2. Il quadro europeo relativo all'identità digitale

Una porzione significativa dei Considerando che fanno da corollario agli articoli del nuovo Regolamento eIDAS si focalizza sul tema dell'istituzione di "*un quadro europeo relativo a un'identità digitale che consenta ai cittadini e ai residenti dell'Unione di accedere a servizi pubblici e privati online e offline in tutta l'Unione*" [Considerando (5)]. L'obiettivo dichiarato è di ridurre "*gli ostacoli digitali tra gli Stati membri e consentendo ai cittadini e ai residenti dell'Unione di godere dei vantaggi della digitalizzazione, aumentando nel contempo la trasparenza e la protezione dei loro diritti.*" [Considerando (6)]. Il nuovo testo sottolinea l'obiettivo di ridurre i rischi e i costi derivanti da soluzioni nazionali tra loro incompatibili, offrendo al contrario un approccio di facile utilizzo e armonizzato che consenta a chiunque di accedere a servizi pubblici e privati in modo sicuro. Il quadro europeo intende quindi superare la logica delle soluzioni di identità digitale di livello nazionale, puntando ad un mezzo di identificazione elettronica armonizzato (il Portafoglio europeo di identità digitale) che consenta non solo l'autenticazione di cittadini e imprese ma anche la fornitura di attestati elettronici di attributi di identità verificati – come qualifiche accademiche o professionali – che siano legalmente riconosciuti in tutta la UE.

Questo quadro armonizzato si pone l'obiettivo di superare gli ostacoli che si sono presentati nell'ambito del riconoscimento e dell'interoperabilità dei mezzi di identificazione elettronica sviluppati negli scorsi anni all'interno dell'Unione, per ridurre i costi operativi legati alle procedure di identificazione e autenticazione elettroniche, promuovendo la trasformazione digitale anche delle piccole e medie imprese dell'Unione e sostenendo la mobilità transfrontaliera.

Un altro aspetto fondamentale deriva dal rispetto dei regolamenti UE in tema di privacy e di trattamento dei dati personali (Regolamento UE 2016/679, Regolamento UE 2018/1725 e Direttiva 2002/58/CE). Si vogliono ad esempio stabilire garanzie volte a separare i dati relativi alla fornitura di servizi di identificazione con quelli di altri servizi erogati dallo stesso fornitore, minimizzando i dati e limitandone le finalità. Secondo gli stessi principi, il Regolamento richiede l'adozione di "*tecnologie che preservino la riservatezza, come ad esempio la dimostrazione a conoscenza zero. Tali metodi crittografici dovrebbero consentire a una parte facente affidamento sulla certificazione di convalidare la veridicità di una determinata dichiarazione sulla base dei dati di identificazione e dell'attestato di attributi della persona in questione, senza rivelare alcun dato su cui si basa tale dichiarazione, così da preservare la vita privata dell'utente.*" [Considerando (14)].

L'obiettivo è di "*proteggere i cittadini e i residenti dell'Unione dall'uso non autorizzato o fraudolento dei portafogli europei di identità digitale al fine di garantire la fiducia negli stessi e la loro ampia diffusione.*" [Considerando (18)].

3. I portafogli europei di identità digitale

La novità più discussa e attesa del nuovo Regolamento eIDAS è l'introduzione di un nuovo modello per l'acquisizione e l'utilizzo di identità digitali basato sui portafogli europei di identità digitale, per consentire agli utenti di identificarsi e autenticarsi a livello transfrontaliero per accedere ad un'ampia gamma di servizi pubblici e privati. Il modello è chiaramente ispirato a quello introdotto con gli "*electronic payment wallet*" (portafogli di pagamento elettronico) dai principali fornitori di dispositivi mobili. Il Regolamento si pone l'obiettivo di fornire ai cittadini europei un portafoglio europeo di identità digitale interamente mobile di facile utilizzo sia online che offline, consentendo ad esempio l'adozione nel settore sanitario dove i servizi sono spesso forniti mediante interazioni faccia a faccia. Il portafoglio di identità digitale, o European Digital Identity Wallet (EDIW), punta a rendere la fruizione dell'identità digitale più semplice, immediata e integrata con gli ecosistemi di servizi pubblici e privati già esistenti o di futura disponibilità, sebbene il Regolamento abbia previsto che il rilascio di identità digitali nel wallet europeo dovrebbe ricorrere "*a mezzi di identificazione elettronica rilasciati a un livello di garanzia elevato*" [Considerando (28)], che potrebbero richiedere un'operatività complicata per un utilizzatore occasionale o non avvezzo all'uso delle tecnologie digitali.

Si sottolinea come l'ampia disponibilità dei portafogli di identità digitale punti ad accrescerne l'accettazione e l'adozione anche nell'ambito dei prestatori di servizi privati. Al Considerando (56) il testo sottolinea come i prestatori nell'ambito dei trasporti, dell'energia, delle banche, della sanità, delle telecomunicazioni e dell'istruzione dovrebbero accettare i wallet di identità digitale laddove la normativa o gli obblighi contrattuali impongano un'autenticazione forte degli utenti. In particolare, alle piattaforme online di grandi dimensioni che richiedono l'autenticazione degli utenti (quelle con oltre 45 milioni di utenti attivi come definiti dal Regolamento 2022/2065, noto anche come "Digital Service Act"), viene imposta l'accettazione degli EDIW quale metodo consentito di autenticazione.

Un richiamo esplicito viene infine fatto all'opportunità che gli Stati membri divulghino i codici sorgenti della propria applicazione utente del wallet, per consentire di comprenderne il funzionamento e di sottoporre il codice a processi di audit, al fine di garantirne la sicurezza, creare fiducia sociale e promuoverne l'accettazione.

4. Attestazione elettronica di attributi

Un'altra importante novità riguarda la definizione di "attributi elettronici". Essi rappresentano un'interessante evoluzione del concetto di identità digitale, che estende il semplice insieme di dati anagrafici – quali nome, luogo e data di nascita, indirizzo di residenza – ad attributi in grado di stabilire una qualifica o uno status particolare, oppure ancora di dimostrare il possesso di un titolo o di un requisito

professionale. I cittadini europei potranno così ad esempio dimostrare di possedere la patente di guida in corso di validità emessa da uno Stato membro, consentendo ad autorità o fornitori di servizi di altri paesi di verificarla con pieno valore giuridico, snellendo procedure di erogazione di servizi ma anche riducendo i rischi di frode. Al proprietario dei dati viene conferito il potere di stabilire quali dati vengano divulgati al soggetto ricevente per la prestazione di un servizio, mediante funzioni intrinseche del wallet che consentano la divulgazione selettiva degli attributi elettronici.

Con la definizione di attributi elettronici arriva anche l'istituzione dei servizi fiduciari di attestazione elettronica di attributi: "*Qualsiasi fornitore di servizi che rilasci attributi in forma elettronica quali diplomi, licenze, certificati di nascita oppure poteri e mandati per rappresentare persone fisiche o giuridiche o agire a loro nome dovrebbe essere considerato un prestatore di servizi fiduciari che fornisce attestati elettronici di attributi.*" [Considerando (55)]. Il Regolamento auspica anche l'adozione di requisiti per garantire gli effetti giuridici degli attestati elettronici qualificati di attributi, da considerarsi equivalenti a quelli degli attestati rilasciati legalmente in forma cartacea. Tuttavia, non sorprenderà che la novità di questo istituto sia accompagnata da un velo di incertezza in merito a normative nazionali, europee o settoriali che potrebbero definire ulteriori requisiti aventi effetti giuridici, sui quali il Regolamento sembra non voler prevalere.

La verifica degli attributi forniti dai prestatori di servizi fiduciari qualificati dovrà avvenire rispetto alle fonti autentiche pertinenti, per le quali il Regolamento prevede l'istituzione di meccanismi che consentano ai prestatori di servizi di verificare l'autenticità degli attributi con il consenso della persona a cui l'attestato viene rilasciato.

In aggiunta ad attributi elettronici emessi da fornitori qualificati, il Regolamento ha previsto anche la possibilità di gestire attributi autocertificati, attribuibili al soggetto che li emette mediante l'utilizzo di firme o sigilli elettronici.

5. Firme elettroniche qualificate gratuite

Sebbene il nuovo testo non stravolga i dettami relativi alle firme elettroniche, sono stati inseriti degli importanti requisiti che riguardano la creazione e l'utilizzo di firme elettroniche qualificate mediante i portafogli di identità digitale. Come previsto dal Considerando (19), "*Una volta effettuato l'onboarding in un portafoglio europeo di identità digitale, le persone fisiche dovrebbero poterlo utilizzare per firmare con firme elettroniche qualificate, per impostazione predefinita e gratuitamente, senza dover sottostare a ulteriori procedure amministrative.*".

Ma la novità più rilevante è che "*L'uso di una firma elettronica qualificata dovrebbe essere gratuito per tutte le persone fisiche a fini non professionali*" mentre "*Gli Stati membri dovrebbero poter prevedere misure che impediscano l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche a fini professionali*"

[Considerando (20)]. Al di là dell'impatto dirompente di un requisito di gratuità sui modelli commerciali finora attuati dai prestatori di servizi qualificati, sul quale il mercato si sta già confrontando in attesa della pubblicazione degli Atti di esecuzione ("Implementing Acts"), si sottolinea come la formulazione del testo non sembra essere particolarmente chiara data l'ambiguità della definizione "persone fisiche a fini professionali", nonché per via della richiesta che gli Stati membri impediscano una modalità operativa che potrebbe invece risultare pienamente adeguata e sostenibile da parte degli operatori del settore.

Il modello di riferimento per la firma elettronica qualificata con il wallet è quello della "firma remota" (anche chiamata *Cloud Signature*), che apre la strada all'adozione su larga scala dello standard aperto promosso dal Cloud Signature Consortium (CSC). I servizi di firma remota prevedono che un fornitore di servizi gestisca i dati per la creazione di una firma qualificata (chiavi crittografiche) per conto del soggetto titolare, con una modalità di erogazione online che semplifica l'esperienza d'uso del firmatario eliminando la complessità della messa a punto del dispositivo di firma. A differenza della prima versione del Regolamento in cui non era previsto, il nuovo testo stabilisce che la gestione conto terzi di dispositivi sicuri di firma (ad esempio gli "*Hardware Security Module*" o HSM) sia considerato un servizio fiduciario a sé stante.

Un punto di novità, già accompagnato da intense discussioni durante la fase di stesura del testo, è il requisito di emissione dei certificati qualificati di firma elettronica mediante identificazione a livello alto, mentre la prima versione del regolamento la consentiva anche con livello sostanziale. L'impatto di questa modifica non è certo trascurabile, dato che in diversi paesi dell'Unione, tra cui l'Italia, la diffusione di identità digitali di livello sostanziale rappresenta una larga maggioranza.

È opportuno sottolineare come nella revisione del Regolamento sia stato posto un accento particolare sull'importanza della verifica dell'identità di persone fisiche o giuridiche per l'erogazione di servizi fiduciari qualificati, al punto da rendere la fase di identificazione ancora più importante di quella di certificazione. Al Considerando (74) si afferma che "*Per garantire che i certificati qualificati e gli attestati elettronici qualificati di attributi siano rilasciati alla persona cui appartengono e che attestino l'insieme corretto e unico di dati che rappresenta l'identità di tale persona, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati o attestati elettronici qualificati di attributi dovrebbero, al momento del rilascio di tali certificati e attestati, garantire con assoluta certezza l'identificazione di tale persona.*", proseguendo poi dettagliando "*il ricorso a mezzi di identificazione elettronica che soddisfano i requisiti del livello di garanzia significativo in combinazione con altri mezzi di verifica dell'identità che consentirebbero di soddisfare i requisiti armonizzati di cui al presente regolamento per quanto riguarda il livello di garanzia elevato nell'ambito di ulteriori procedure armonizzate a distanza, garantendo l'identificazione con un elevato livello di affidabilità.*".

Un altro interessante spunto deriva dal Considerando (63) in cui il testo, pur riconoscendo che gli effetti giuridici delle firme elettroniche siano di competenza del

diritto nazionale, indica che "*gli Stati membri dovrebbero tenere conto del principio di proporzionalità tra il valore giuridico di un documento da firmare e il livello di sicurezza e di costo richiesto da una firma elettronica. Per aumentare l'accessibilità e l'uso delle firme elettroniche, gli Stati membri sono incoraggiati a valutare l'uso di firme elettroniche avanzate nelle transazioni quotidiane, per le quali essi forniscono un livello sufficiente di sicurezza e affidabilità*.". Questa formulazione un po' sorprende non solo dato l'approccio privilegiato verso le firme elettroniche qualificate presente nel Regolamento, ma anche perché gli aspetti di sicurezza e affidabilità delle firme elettroniche avanzate non sono stati finora formulati attraverso atti implementativi specifici o pratiche di certificazione.

6. Certificati qualificati per l'autenticazione di siti Web

Un tema controverso e sostanzialmente disatteso del primo Regolamento eIDAS è certamente quello dei certificati qualificati per autenticazione web, anche detti QWAC (Qualified Web Authentication Certificates). Alcune polemiche si sono accese negli anni passati tra i fornitori di servizi fiduciari accreditati per l'emissione di tali certificati e alcuni membri del CABF (CA/Browser Forum), che regolamenta il mercato dei certificati di autenticazione web (TLS) mediante funzionalità e liste di fiducia (Trust List) che consentono di stabilire se un sito web visitato sia da ritenersi affidabile o meno, in virtù dell'origine e integrità dei suoi contenuti. Negli anni passati tali polemiche hanno sostanzialmente limitato il mercato dei certificati QWAC, la cui adozione per altro non è obbligatoria, sebbene essi siano richiesti per alcuni casi d'uso specifici, come la conformità alla seconda Direttiva europea sui servizi di pagamento o Payment Service Directive (PSD2).

Senza entrare nel merito di queste polemiche, si sottolinea come il nuovo Regolamento rafforzi il ruolo dei certificati QWAC stabilendo che "*Il riconoscimento dei certificati qualificati di autenticazione di siti web comporta che i fornitori di browser web non dovrebbero negare l'autenticità dei certificati qualificati di autenticazione di siti web al solo scopo di attestare il collegamento tra il nome di dominio del sito web e la persona fisica o giuridica a cui è rilasciato il certificato o di confermare l'identità di tale persona*.". E ancora, "*I fornitori di browser web dovrebbero far sì che l'utente finale visualizzi i dati di identità certificati e gli altri attributi in modo facilmente consultabile nell'ambiente del browser, tramite mezzi tecnici di loro scelta*." [Considerando (65)]. In pratica, i web browser devono garantire il supporto dei certificati qualificati di autenticazione web emessi secondo il Regolamento. Si auspica che gli atti di esecuzione in questo ambito forniscano i chiarimenti tecnici necessari a scongiurare pericolose contrapposizioni tra operatori del mercato e istituzioni europee.

7. Archiviazione elettronica qualificata

Il nuovo Regolamento stabilisce anche un nuovo quadro giuridico per i servizi di archiviazione elettronica qualificati, ispirato a quello di altri servizi fiduciari definiti in eIDAS. Questo quadro giuridico dovrebbe offrire ai prestatori di servizi fiduciari e agli utenti uno strumento efficiente per i servizi di archiviazione elettronica, nonché chiari effetti giuridici quando viene utilizzato un servizio di archiviazione elettronica qualificato. Tali disposizioni si applicano ai dati elettronici e ai documenti elettronici creati in forma elettronica, nonché ai documenti cartacei che sono stati scansionati e digitalizzati. L'archiviazione elettronica qualificata viene specificata non solo come mero "*storage* affidabile", ma soprattutto come sistema in grado di conservare a lungo termine la memoria elettronica comprensiva degli elementi accessori quali firme elettroniche e sigilli, ovvero validazioni temporali elettroniche.

Tale novità nasce dal tentativo di risolvere una situazione attuale abbastanza frammentata e connotata da assoluta mancanza di interoperabilità tra servizi di archiviazione di livello nazionale. Tali servizi finora si sono sviluppati sulla base di specifici regolamenti nazionali che hanno precluso non solo la libera circolazione dei fornitori di servizi intracomunitari, ma soprattutto l'impossibilità di fruire di servizi omogenei forniti da operatori accreditati in paesi membri differenti.

8. Registri elettronici

Il nuovo eIDAS introduce anche i libri mastri elettronici qualificati, per stabilire una presunzione legale di ordine cronologico sequenziale unico e accurato e di integrità dei dati registrati nel libro mastro. Questa novità prende spunto dalla diffusione dei "*distributed ledger*" ovvero i sistemi basati su tecnologia blockchain, sebbene il Regolamento precisi ancora la sua neutralità tecnologica, ovvero non favorisca né discrimini alcuna tecnologia utilizzata per realizzare il nuovo servizio fiduciario per i registri elettronici. Il testo piuttosto si avventura nell'esemplificazione di alcuni casi d'uso che ne giustificano la comparsa nel Regolamento: il voto elettronico, la cooperazione transfrontaliera delle autorità doganali, la cooperazione transfrontaliera delle istituzioni accademiche e la registrazione delle proprietà immobiliari nei registri catastali decentrati.

L'aspetto importante è che anche in questo caso viene richiesta l'istituzione di "*un quadro giuridico a livello dell'Unione che disponga il riconoscimento transfrontaliero dei servizi fiduciari per la registrazione dei dati nei registri elettronici. Ciò dovrebbe impedire in misura sufficiente che lo stesso bene digitale sia copiato e venduto più di una volta a diverse parti.*" [Considerando (68)].

9. Conclusioni

Un ultimo aspetto che si vuole evidenziare sono i benefici dei servizi fiduciari definiti dal Regolamento, che stanno acquisendo una sempre maggiore importanza per il commercio e la cooperazione internazionali. Diversi paesi al di fuori dell'Unione Europea stanno istituendo o definendo quadri normativi che si ispirano al Regolamento eIDAS. La Commissione Europea viene quindi stimolata ad adottare atti di esecuzione per stabilire le condizioni per l'equivalenza giuridica con gli schemi adottati da paesi terzi, al fine di ottenere il riconoscimento reciproco dei servizi fiduciari e dei relativi prestatori. Questo aspetto avrà anche un ruolo importante nel panorama delle relazioni e delle alleanze internazionali, sempre più impattate dalle comunicazioni digitali.

È infine importante precisare che il Regolamento eIDAS mantiene un livello di neutralità tecnologica e indica alla Commissione Europea l'adozione di atti di esecuzione che stabiliscano elenchi di norme e standard per determinare specifiche e procedure operative, nonché i requisiti per le certificazioni di conformità. Entro i 12/24 mesi successivi alla pubblicazione in Gazzetta Ufficiale è prevista la pubblicazione di ben 47 atti di esecuzione prima che il nuovo Regolamento possa entrare pienamente in vigore.

Tali atti entreranno nel merito degli aspetti implementativi, anche referenziando standard e norme tecniche che avranno quindi un impatto fondamentale nello sviluppo delle tecnologie e dei servizi per attuare quanto previsto dal Regolamento. Per questo motivo gli enti normativi europei CEN, CENELC e ETSI sono al lavoro da tempo, e ci sarà ancora molto da scoprire in merito agli aspetti tecnologici.

N. 4 - 2024 - pp. 20-31

Il regolamento eIDAS n. 2024/1183 ed il Codice dell'amministrazione digitale. Alcune considerazioni su modifiche ed integrazioni.

Donato A. Limone

Abstract [IT]: Considerazioni sul regolamento EU n.2024/1183 sulla identità digitale e il portafoglio dei servizi digitali.

Abstract [EN]: Considerations on the EU regulation n.2024/1183 on digital identity and Wallet digital services.

Parole chiave: identità digitale; identità digitale europea; portafoglio dei servizi digitali; attributi elettronici.

Sommario: 1. La modifica del regolamento eIDAS n.910/2014 con il regolamento 2024/1183 – 2. Il contesto normativo di eIDAS/2: il quadro europeo unitario sulla identità digitale e il portafoglio dei servizi – 3.Il regolamento eIDAS/2 (2024/1183). Modifiche del Codice dell'amministrazione digitale – 4. Alcune conclusioni.

1. La modifica del regolamento eIDAS n.910/2014 con il nuovo regolamento 2024/1183

Il regolamento UE 2024/1183 (di seguito indicato come eIDAS/2) modifica il regolamento UE 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a *un'identita digitale* (eIDAS - electronic Identification Authentication and Signature) e al *portafoglio digitale* dei servizi basato appunto sulla identità digitale unica, sicura e interoperabile. La modifica opera una *sintesi organica* tra identità digitale e portafoglio digitale dei servizi "rivoluzionando" il sistema dei servizi digitali, identità digitali, i mercati in rete. Faremo quindi alcune considerazioni tra queste novità particolarmente rilevanti ed il nostro *Codice dell'amministrazione*

digitale che in modo organico ha trattato di identità digitale, di accessibilità in rete, di valore legale dei documenti informatici e delle firme elettroniche, della interoperabilità, dei requisiti dei dati digitali, della conservazione dei documenti, dei servizi pubblici digitali, di cittadinanza digitale e nuovi diritti digitali. *Codice* che per primo nel mondo ha affrontato con un approccio sistemico e globale tutta la materia relativa al digitale pubblico in particolare. Come l'ordinamento italiano aveva regolato nel 1997 il valore legale del documento informatico e delle firme elettroniche (in particolare la firma digitale; vedi la legge 59 del 1997; poi il Dpr 513/97). Ma con la legge 191/1998, art.2 aveva anche normato in tema di *carta di identità elettronica; di lavoro digitale* (art. 4 della legge 191/1998). Tutti temi che (trascurati alcuni nella fase di applicazione) ritorneranno all' attenzione delle istituzioni, della politica, del sistema sociale ed economico sia con il regolamento eIDAS 910/2014, sia con la legge 124/2015 (Carta della cittadinanza digitale) sia con il Covid che ha "riproposto" per necessità i temi della identità digitale, del valore legale dei dati/documenti, delle transazioni elettroniche nel settore pubblico e privato. Fino alla modifica apportata con eIDAS/2 (2024/1183). Tutti temi e modifiche che ha visto in prima fila (e in anticipo) il nostro Paese.

2. Il contesto normativo di eIDAS/2: il quadro europeo unitario sulla identità digitale e il portafoglio dei servizi

Per considerare la portata di questa modifica è necessario fare un breve riferimento al contesto normativo nel quale viene approvato eIDAS/2. Il contesto normativo è caratterizzato da una costante legislazione della Unione che, rispetto al processo di trasformazione digitale, valorizza da un lato i principi del mercato interno e dall'altro le esigenze di tutela dei diritti e delle libertà fondamentali della persona. Mi limito a fare riferimento al regolamenti 2022/868 (*Data Governance Act*), 2022/1925 (*Digital Markets Act*), 2022/2065 (*Digital Services Act*), sulla IA. E per gli aspetti generali e di "cornice" faccio riferimento alla *"Dichiarazione europea sui diritti e i principi digitali per il decennio digitale"* (2023). Un contesto particolarmente innovativo. La citata normativa in particolare si fonda sul rapporto tra "identità elettronica" e "servizi digitali" tramite le "transazioni elettroniche". I considerando hanno la funzione di "inquadrare" i temi che poi sono normati nel testo del regolamento; nei primi "considerando" del regolamento i principi ed i concetti-guida della normativa europea sulla identità digitale.

Un quadro europeo per la identificazione elettronica pubblica e sicura: La modifica del regolamento 910/2014 è stata annunciata nella comunicazione della Commissione del 19 febbraio 2020 intitolata «Plasmare il futuro digitale dell'Europa» al fine di migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere

identità digitali affidabili per tutti gli europei. "Nelle sue conclusioni dell'1-2 ottobre 2020, il Consiglio europeo ha chiesto alla Commissione di proporre lo sviluppo di un quadro a livello dell'UE per l'identificazione elettronica pubblica e sicura, ivi incluse le firme digitali interoperabili, che garantisca alle persone il controllo della loro identità e dei loro dati online e consenta l'accesso a servizi digitali pubblici, privati e transfrontalieri" (*Considerando 2*).

Un programma per la diffusione di una identità digitale: Il programma strategico per il decennio digitale 2030, istituito dalla decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio , "stabilisce le finalità e gli obiettivi digitali di un quadro dell'Unione che dovrebbero condurre entro il 2030 a un'ampia diffusione di un'identità digitale affidabile, volontaria e controllata dagli utenti che sia riconosciuta in tutta l'Unione e consenta a ciascun utente di controllare i propri dati nelle interazioni online" (*Considerando 3*).

Diritto di accesso a tecnologie, prodotti e servizi: Nella «dichiarazione europea sui diritti e i principi digitali per il decennio digitale», proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione, si sottolinea il diritto di ogni persona di avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione. "Ciò include la garanzia che a tutte le persone che vivono nell'Unione sia offerta un'identità digitale accessibile, sicura e affidabile che dia accesso a un'ampia gamma di servizi online e offline, protetti contro i rischi di cibersicurezza e la criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità. La dichiarazione stabilisce inoltre che ogni persona ha diritto alla protezione dei propri dati personali. Tale diritto comprende il controllo su come i dati sono utilizzati e con chi sono condivisi" (*Considerando 4*).

Identità digitale sotto il controllo dei cittadini: "I cittadini e i residenti dell'Unione dovrebbero avere il diritto a un'identità digitale che sia sotto il loro controllo esclusivo e che consenta loro di esercitare i propri diritti nell'ambiente digitale e di partecipare all'economia digitale. Per conseguire tale obiettivo è opportuno istituire un quadro europeo relativo a un'identità digitale che consenta ai cittadini e ai residenti dell'Unione di accedere a servizi pubblici e privati online e offline in tutta l'Unione (*Considerando 5*).

L'identità digitale per una Unione più integrata: "Un quadro armonizzato relativo all'identità digitale contribuirebbe alla creazione di un'Unione più integrata dal punto di vista digitale, riducendo gli ostacoli digitali tra gli Stati membri e consentendo ai cittadini e ai residenti dell'Unione di godere dei vantaggi della digitalizzazione, aumentando nel contempo la trasparenza e la protezione dei loro diritti" (*Considerando 6*).

Superamento della frammentazione normativa; rafforzamento del mercato interno; un portafoglio europeo di identità digitale; attributi validi in tutta Europa: "Un approccio maggiormente armonizzato all'identificazione elettronica dovrebbe ridurre i rischi e i costi dell'attuale frammentazione dovuta all'uso di soluzioni nazionali divergenti oppure, in alcuni Stati membri, all'assenza di tali soluzioni di identificazione elettronica. Un tale approccio dovrebbe rafforzare il mercato interno consentendo ai cittadini e ai residenti dell'Unione, quali definiti dalle legislazioni nazionali, e alle imprese di identificarsi e di fornire un'autenticazione della propria identità online e offline in modo sicuro, affidabile, di facile utilizzo, pratico, accessibile e armonizzato in tutta l'Unione. Il portafoglio europeo di identità digitale dovrebbe fornire alle persone fisiche e giuridiche di tutta l'Unione un mezzo di identificazione elettronica armonizzato che consenta l'autenticazione e la condivisione dei dati collegati alla loro identità. Tutti dovrebbero poter accedere a servizi pubblici e privati in modo sicuro, sulla base di un ecosistema migliorato per i servizi fiduciari e su prove dell'identità e attestati elettronici di attributi verificati, come qualifiche accademiche, compresi diplomi universitari o altri titoli di studio o qualifiche professionali. Il quadro europeo relativo a un'identità digitale è inteso consentire il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi e legalmente riconosciuti in tutta l'Unione. I fornitori di attestati elettronici di attributi dovrebbero beneficiare di un insieme di norme chiaro e uniforme, mentre le amministrazioni pubbliche dovrebbero potersi avvalere di documenti elettronici in un formato prestabilito" (*Considerando 7*).

Valorizzazione dei diversi regimi di identità digitale e rapida adozione dei portafogli europei di identità digitale: "Vari Stati membri hanno attuato e utilizzano mezzi di identificazione elettronica che sono accettati dai prestatori di servizi nell'Unione. Inoltre sono stati effettuati investimenti in soluzioni sia nazionali che transfrontaliere sulla base del regolamento (UE) n. 910/2014, compresa l'interoperabilità dei regimi di identificazione elettronica notificati ai sensi di tale regolamento. Al fine di garantire la complementarità e una rapida adozione dei portafogli europei di identità digitale da parte degli attuali utenti di mezzi di identificazione elettronica notificati e di ridurre al minimo l'impatto sui prestatori di servizi esistenti, i portafogli europei di identità digitale dovrebbero trarre vantaggio dall'esperienza acquisita con i mezzi di identificazione elettronica esistenti e dall'infrastruttura dei regimi di identificazione elettronica notificati utilizzati a livello dell'Unione e nazionale" (*Considerando 8*).

Applicazione della normativa in materia di protezione dei dati personali nei portafogli digitali (considerando 9):
"Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio si applicano a tutte le attività di trattamento dei dati personali ai sensi del regolamento (UE) n. 910/2014. Anche le soluzioni nell'ambito del quadro di interoperabilità di cui al pre-

sente regolamento sono conformi a tali norme. La normativa dell'Unione in materia di protezione dei dati stabilisce principi di protezione dei dati, quali la minimizzazione dei dati e il principio di limitazione delle finalità, e obblighi in materia, ad esempio la protezione dei dati fin dalla progettazione e per impostazione predefinita".

L'attuale regolamento quindi stabilisce le condizioni armonizzate per un quadro unitario sulle identità digitali; i diritti dei cittadini e dei residenti della Unione; i dati personali; identità digitali e società democratiche; accesso a tecnologie sicure; parità di accesso alle identità: "Il presente regolamento stabilisce le condizioni armonizzate per l'istituzione di un quadro per i portafogli europei di identità digitale che saranno forniti dagli Stati membri. Tutti i cittadini e i residenti dell'Unione quali definiti dal diritto nazionale dovrebbero poter richiedere, selezionare, combinare, conservare, cancellare, condividere e presentare in sicurezza i dati relativi alla loro identità e richiedere la cancellazione dei loro dati personali in modo pratico e intuitivo, con il controllo esclusivo dell'utente, consentendo al contempo la divulgazione selettiva dei dati personali. Il presente regolamento riflette i valori europei condivisi e rispetta i diritti fondamentali, le garanzie giuridiche e la responsabilità, proteggendo in tal modo le società democratiche, i cittadini e i residenti dell'Unione. Le tecnologie utilizzate per conseguire tali obiettivi dovrebbero essere sviluppate cercando di ottenere il massimo livello di sicurezza, riservatezza, praticità per gli utenti, accessibilità, ampia utilizzabilità e interoperabilità senza soluzione di continuità. Gli Stati membri dovrebbero garantire a tutti i loro cittadini e residenti la parità di accesso all'identificazione elettronica. Gli Stati membri non dovrebbero limitare, direttamente o indirettamente, l'accesso a servizi pubblici o privati da parte di persone fisiche o giuridiche che scelgono di non utilizzare i portafogli europei di identità digitale e dovrebbero mettere a disposizione soluzioni alternative adeguate." (*Considerando 15*).

Prestatori di servizi; soluzioni di identità digitale riconosciute dalla Unione; valore giuridico degli attestati elettronici di attributi; quadro giuridico unitario per creare valore economico: "Al fine di sostenere la competitività delle imprese dell'Unione, i prestatori di servizi sia online che offline dovrebbero potersi avvalere di soluzioni di identità digitale riconosciute in tutta l'Unione, indipendentemente dallo Stato membro in cui tali soluzioni sono fornite, traendo in tal modo vantaggio da un approccio armonizzato a livello dell'Unione in materia di fiducia, sicurezza e interoperabilità. Sia gli utenti che i prestatori di servizi dovrebbero poter beneficiare in tutta l'Unione dello stesso valore giuridico conferito agli attestati elettronici di attributi. Un quadro armonizzato in materia di identità digitale ha l'obiettivo di creare valore economico fornendo un accesso più agevole a beni e servizi e riducendo in modo significativo i costi operativi legati alle procedure di identificazione e autenticazione elettroniche, ad esempio durante l'onboarding (acquisizione) di nuovi clienti, riducendo il rischio di reati informatici, quali furto di identità, furto di dati e frodi online, così da favorire guadagni in termini di efficienza e promuovere la

trasformazione digitale sicura delle microimprese e delle piccole e medie imprese (PMI) dell'Unione" (*Considerando 10*).

Il principio "una tantum"; riduzione oneri amministrativi: "I portafogli europei di identità digitale dovrebbero facilitare l'applicazione del principio «una tantum», in modo da ridurre gli oneri amministrativi e sostenere la mobilità transfrontaliera per i cittadini e i residenti dell'Unione e le imprese in tutta l'Unione e promuovere lo sviluppo di servizi interoperabili di e-government in tutta l'Unione" (*Considerando 11).*

3. Il regolamento eidas/2 (2024/1183). Modifiche del Codice dell'amministrazione digitale

Non intendiamo fare un'analisi specifica dei considerando (sono 78) ma vogliamo fare considerazioni su alcuni principi, concetti, aspetti che sono alla base dei considerando e del testo del regolamento 910/2014 modificato (gli articoli del regolamento modificato sono 2: l'articolo 1 riporta tutte le modifiche al regolamento 910/2014; l'articolo 2 stabilisce l'entrata in vigore del regolamento). Intendiamo fare alcune considerazioni sul testo del regolamento anche in corrispondenza con il testo del *Codice dell'amministrazione*. Il regolamento eIDAS/2 modifica ed integra il regolamento 910/2014 che resta quindi in vigore.

L'oggetto del regolamento modificato (2024/1183) è quindi stabilito con la sostituzione dell'art. 1 del 910/2014: *"Il presente regolamento mira a garantire il buon funzionamento del mercato interno e a fornire un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari utilizzati in tutta l'Unione, al fine di consentire e facilitare l'esercizio, da parte delle persone fisiche e giuridiche, del diritto di partecipare in modo sicuro alla società digitale e di accedere ai servizi pubblici e privati online in tutta l'Unione. A tal fine, il presente regolamento:*

1. *a) fissa le condizioni alle quali 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 e forniscono e riconoscono i portafogli europei di identità digitale;*
2. *b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;*
3. *c) istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato, i servizi relativi ai certificati di autenticazione di siti web, l'archiviazione elettronica, gli attestati elettronici di*

attributi, i dispositivi per la creazione di una firma elettronica, i dispositivi per la creazione di sigilli elettronici e i registri elettronici.»; [……..].

L'art. 1 quindi definisce *nuove finalità* del regolamento in considerazione del mercato interno, della sicurezza dei servizi fiduciari, dell'esercizio del diritto da parte delle *persone fisiche e giuridiche* di partecipare in modo *sicuro* alla società digitale e di accedere ai servizi pubblici e privati on line in tutta l'Unione. Un quadro delle finalità articolato, in linea con un quadro unitario europeo delle norme valido per tutti i Paesi membri. Un quadro di finalità che modifica quindi il quadro delle condizioni di riconoscimento e di accesso ai servizi fiduciari con il riconoscimento dei "portafogli europei di identità digitale". Il regolamento istituisce un quadro giuridico più articolato rispetto al 910/2014 per quanto riguarda firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi di recapito elettronico, ecc.

Il regolamento 2024/1183 introduce alcune novità importanti:

a) la definizione di un *quadro unitario completo*, come abbiamo già rilevato;
b) la sistematizzazione concettuale *dell'apparato definitorio*;
c) l'introduzione del *"portafoglio digitale".*

Consideriamo ora l'apparato definitorio. Osserviamo subito che sarà necessario integrare/modificare l'apparato definitorio del nostro Codice dell'amministrazione digitale (art. 1bis): "Ai fini del presente Codice, valgono le definizioni di cui all'art. 3 del Regolamento eIDAS; [……..]. Infatti, sarà necessario riportare nel *Codice* le modifiche dell'art. 2 del regolamento 910/2014, come modificato dal regolamento 2024/1183.

Le modifiche e le integrazioni delle definizioni riguardano l'art. 3 reg. 2024/1183 (in corsivo il testo modificato che sottolineamo):

- i punti da 1) a 5) sono sostituiti dalle definizioni di "identificazione elettronica" (parte modificata:…..*una persona fisica che rappresenta un'altra persona fisica o una persona giuridica*), "mezzi di identificazione elettronica" (parte modificata:……*o se del caso per un servizio offline*), "dati di identificazione personale" (parte modificata:……*che rappresenta un'altra persona fisica o una persona giuridica*) , "regime di identificazione elettronica" (parte modificata:……o *alle persone fisiche che rappresentano persone fisiche o persone giuridiche*) , "autenticazione" (parte modificata:….. *oppure confermare l'origine e l'integrità di dati in forma elettronica).*
- Nel punto 5 bis si introduce il termine *"utente":* "utente", una persona fisica o giuridica, o una persona fisica che rappresenta un'altra persona fisica o una persona giuridica, che utilizza servizi fiduciari o mezzi di identificazione elettronica, forniti a norma del presente regolamento;».
- Punto 6 sostituito: "parte facente affidamento sulla certificazione", una

persona fisica o giuridica che fa affidamento sull'identificazione elettronica, sui portafogli europei di identità digitale o su altri mezzi di identificazione elettronica, oppure su un servizio fiduciario».

- Il punto 16 relativo alla definizione di *"servizio fiduciario"* è sostituito da un testo più articolato che si riferisce alle novità del regolamento 2024/1183: un quadro organico sui servizi fiduciari; identità certa e sicura; attributi; il portafoglio digitale. Nel punto 16 è definito il servizio fiduciario rispetto ai suoi elementi costitutivi (il corsivo è nostro):
- a) il *rilascio di certificati* di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; b) la *convalida di certificati* di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; c) la *creazione* di firme elettroniche o sigilli elettronici; d) la *convalida* di firme elettroniche o sigilli elettronici; e) la *conservazione* di firme elettroniche, sigilli elettronici, certificati di firme elettroniche o certificati di sigilli elettronici; f) la *gestione di dispositivi* per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza; g) il rilascio di *attestati elettronici di attributi*; h) la *convalida* di attestati elettronici di attributi; i) la creazione di *validazioni temporali elettroniche*; j) la *convalida* di validazioni temporali elettroniche; k) la prestazione di servizi elettronici di *recapito certificato*; l) la *convalida* dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove; m) *l'archiviazione elettronica* di dati elettronici e di documenti elettronici; n) la registrazione di dati elettronici in un *registro elettronico*".

- Dopo il punto 41 nel nuovo regolamento sono inseriti *16 punti nuovi importanti* relativi al *portafoglio europeo di identità digitale* non previsto e non regolato dal regolamento 910/2014:
- «42) "*Portafoglio europeo di identità digitale*", un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati; 43) *"attributo",* la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto; 44) *"attestato elettronico di attributi"*, un attestato in forma elettronica che consente l'autenticazione di attributi; 45) *"attestato elettronico di attributi qualificato",* un attestato elettronico di attributi che è rilasciato da un prestatore di servizi fiduciari qualificato e soddisfa i requisiti di cui all'allegato V; 46) *"attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto"*, un attestato elettronico di attributi

rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o da un organismo del settore pubblico designato dallo Stato membro per rilasciare tali attestati di attributi per conto di organismi del settore pubblico responsabili di fonti autentiche in conformità dell'articolo 45 septies e che soddisfa i requisiti di cui all'allegato VII; 47) *"fonte autentica",* un archivio o un sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o di un soggetto privato, che contiene e fornisce gli attributi relativi a una persona fisica o giuridica o a un oggetto e che è considerato una fonte primaria di tali informazioni o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa; 48) *"archiviazione elettronica",* un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione; 49) *"servizio di archiviazione elettronica qualificato"*, un servizio di archiviazione elettronica fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 undecies; 50) *"marchio di fiducia UE per i portafogli di identità digitale"*, un'indicazione verificabile, semplice e riconoscibile, comunicata in modo chiaro, del fatto che un portafoglio europeo di identità digitale è stato fornito conformemente al presente regolamento; 51) *"autenticazione forte dell'utente",* un'autenticazione basata sull'uso di almeno due fattori di autenticazione appartenenti a diverse categorie, della conoscenza qualcosa che solo l'utente conosce, del possesso, qualcosa che solo l'utente possiede, o dell'inerenza, qualcosa che caratterizza l'utente, che sono indipendenti, in modo tale che la violazione di uno degli elementi non comprometta l'affidabilità degli altri, e progettata in maniera tale da proteggere la riservatezza dei dati di autenticazione; 52) *"registro elettronico",* una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni; 53) *"registro elettronico qualificato*", un registro elettronico fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 terdecies; 54) *"dati personali*", qualsiasi informazione quale definita all'articolo 4, punto 1, del regolamento (UE) 2016/679; 55) *"corrispondenza dell'identità*", un processo in cui i dati di identificazione personale o i mezzi di identificazione elettronica sono abbinati o collegati a un account esistente appartenente alla stessa persona; 56) *"registrazione di dati*", dati elettronici registrati con i metadati connessi che supportano il trattamento dei dati; 57) *"modalità offline*", per quanto riguarda l'uso dei portafogli europei di identità digitale, un'interazione tra un utente e un terzo in un luogo fisico per mezzo di tecnologie di prossimità, laddove il portafoglio europeo di identità digitale non è tenuto ad accedere a sistemi a distanza tramite reti di comunicazione elettronica

ai fini dell'interazione».

- La *sezione 1* del regolamento si occupa del *"Portafoglio europeo di identità digitale"*. La sezione comprende: Portafogli europei di identità digitale (art. 5 bis); Parti facenti affidamento sulla certificazione dei portafogli europei di identità digitale (art. 5 ter); Certificazione dei portafogli europei di identità digitale (art. 5 quater); Pubblicazione di un elenco dei portafogli europei di identità digitale certificati (art. 5 quinquies); Violazione della sicurezza dei portafogli europei di identità digitale (art. 5 sexies); Ricorso transfrontaliero ai portafogli europei di identità digitale (Art. 5 septies).

- La sezione 2 del regolamento si occupa dei *"Regimi di identificazione elettronica"*.
  In questa sezione sono inseriti diversi articoli che regolamentano il regime di identificazione elettronica: l'articolo 11 bis (*Corrispondenza dell'identità a livello transfrontaliero*); articolo 12 bis (*Certificazione dei regimi di identificazione elettronica*); articolo 12 ter (*Accesso a componenti hardware e software*); articolo 14,15 e 16 sono sostituiti con art. 14 (*Aspetti internazionali*); art. 15 (*Accessibilità per le persone con disabilità ed esigenze particola*ri); art. 16 (*Sanzioni)*.
  Sono inseriti l'art. 19 bis (*Requisiti per i prestatori di servizi fiduciari non qualificati*); l'art. 24 bis (*Riconoscimento dei servizi fiduciari qualificati*); l'art. 29 (*Requisiti relativi ai servizi qualificati per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza);* l'art. 32 bis (*Requisiti per la convalida delle firme elettroniche avanzate basate su certificati qualificati);* l'art. 39 bis (*Requisiti relativi ai servizi qualificati per la creazione di un sigillo elettronico a distanza)*; art. 40 bis *(Requisiti per la convalida dei sigilli elettronici avanzati basati su certificati qualificati);* art. 45 (*Requisiti per i certificati qualificati di autenticazione di siti web)*; art. 45 bis (*Misure precauzionali in materia di cibersicurezza*).

- Nella sezione 9 (*Attestati elettronici di attributi*) sono compresi l'art. 45 ter (*Effetti giuridici degli attestati elettronici di attributi)*; art. 45 quater (*Attestati elettronici di attributi nei servizi pubblici);* art. 45 quinquies (*Requisiti per gli attestati elettronici qualificati di attributi*); art. 45 sexies (*Verifica degli attributi rispetto a fonti autentiche)*; art. 45 septies (Requisiti per gli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto); art. 45 octies(Rilascio di attestati elettronici di attributi ai portafogli europei di identità digitale); art. 45 nonies (Norme supplementari per la prestazione di servizi di attestazione elettronica di attributi).

- Nella sezione 10 (*Servizi di archiviazione elettronica*) sono compresi l'art.

45 decies (Effetti giuridici dei servizi di archiviazione elettronica); art. 45 undecies (Requisiti per i servizi di archiviazione elettronica qualificati).

- La sezione 11 del regolamento è dedicata ai *Registri elettronici:* con l'art. 45 duodecies (Effetti giuridici dei registri elettronici) e l'art. 45 terdecies (Requisiti per i registri elettronici qualificati).

- Nel Capo IV bis (Quadro di Governance) sono compresi l'art. 46 bis (Vigilanza sul quadro relativo al portafoglio europeo di identità digitale); art. 46 ter (Vigilanza dei servizi fiduciari); art. 46 quater (Punti di contatto unici); art. 46 quinquies (Assistenza reciproca); art. 46sexies (Gruppo di cooperazione per l'identità digitale europea).
  Nel capo VI è inserito l'art. 48 bis (Obblighi di comunicazione).
  L'applicazione del regolamento sarà riesaminata entro il 21 maggio 2026.
  Una annotazione sull'allegato V (Requisiti per gli attestati elettronici qualificati di attributi): sono elencati gli attestati. L'allegato VI riporta l'elenco minimo di attributi. L'allegato VII comprende i requisiti per gli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto.

4. Alcune conclusioni

Questo mio contributo trova una serie di riscontri, di applicazioni, di risposte negli articoli "tecnici" pubblicati in questo volume (tutti contributi di alto livello) ed in particolare negli articoli di Giovanni Manca.
Come procedere nell'applicazione del Regolamento eIDAS/2 nel nostro Paese?

Primi suggerimenti.

Il Regolamento impegnerà Governo, amministrazioni pubbliche, specialisti, mercati.
Il Governo dovrebbe intervenire, attraverso le proprie strutture delegate alla trasformazione digitale, per:

a) Modificare/integrare il *Codice dell'amministrazione digitale* nelle parti che hanno a che fare con le definizioni, la identità digitale, con le firme elettroniche, con la conservazione e l'archiviazione dei documenti, il portafoglio digitale dei servizi.
b) Le definizioni del regolamento eIDAS/2 costituiscono la *intelaiatura concettuale* di base di una parte nuova del *Codice* stesso (da scrivere): un Codice sempre più aperto verso i servizi digitali, le transazioni elettroniche, l'accessibilità ai sistemi, la interoperabilità dei sistemi dei dati e delle

tecnologie, i vari livelli di sicurezza informatica, sia nel settore pubblico e sia in quello privato.

c) Per definire un primo quadro di *regole tecniche* finalizzato alla realizzazione di portafogli digitali di servizi.
d) Per attivare *progetti di portafoglio* dei servizi digitali pubblici.

La sezione II del *Codice* (Diritti dei cittadini e delle imprese: art. 3-11) dovrà essere necessariamente riconsiderata alla luce del Regolamento per quanto attiene i servizi ai cittadini e alle imprese.

L'art. 3 bis (identità digitale e domicilio digitale), l'art. 6 (utilizzo del domicilio digitale) sono da riconsiderare in ragione del Regolamento.

L'art. 7 del *Codice* (Servizi in rete) dovrebbe essere riconsiderato per quanto attiene ai servizi digitali nell'ottica del portafoglio digitale dei servizi.

Con riferimento al regolamento sarà necessario fare una riconsiderazione complessiva sulle firme elettroniche, sui sigilli elettronici, sui registri elettronici, sui siti web, sui servizi in rete, sulle modalità di accedere ai siti per presentare istanze e dichiarazioni, ecc.

Una parte del *Codice* dovrebbe assimilare e comprendere tutti i principi relativi ai portafogli digitali.

L'utilizzo degli *attributi personali elettronici* con sistemi elettronici sicuri di identità digitale (CIE) permetterebbe una fortissima riduzione di certificazioni analogiche fornite dalle pubbliche amministrazioni per poi presentare istanze e richieste e quindi una forte limitazione del fenomeno della ridondanza di dati, documenti e procedure burocratiche sulla base del principio "una sola volta" o "una tantum". Uno snellimento burocratico formidabile che permetterebbe di chiudere quasi completamente la fase delle *burocrazie analogiche* dove tutto era (ed è ancora) basato su di un circuito "non virtuoso" costituito da dichiarazioni dei cittadini su dati, fatti e qualità forniti alla burocrazia che dalla stessa burocrazia, con una finzione formalistica (verifica dei dati dichiarati sempre gli stessi "n" volte), sono quindi resi validi e sicuri. La chiusura di questa "burocrazia analogica per autodichiarazioni" finalmente permetterebbe l'avvio di una burocrazia nativamente digitale, semplificata e valida, accessibile in rete.

N. 4 - 2024 - pp. 32-41

Il regolamento eIDAS 2.0 e l'impatto sulla gestione documentale delle PA: quali prospettive?

Ernesto Belisario

Abstract [IT]: *Il Regolamento eIDAS (Reg. Ue n. 910/2014) costituisce a livello europeo il quadro giuridico di riferimento per la regolazione dei servizi fiduciari elettronici, tra cui quelli relativi alla formazione, gestione e conservazione dei documenti informatici. Nell'atto di modifica al Regolamento (Reg. UE 2024/1183, c.d. "eIDAS 2.0"), si prevede un notevole ridimensionamento dell'attuale sistema di qualificazione dei fornitori di tali servizi, sopperito da massiccio rinvio, per il tramite degli atti di esecuzione del Regolamento, a norme tecniche e standard sovranazionali. Ciò dovrebbe comportare una significativa deregolamentazione della materia e, al contempo, una notevole apertura del mercato di tali servizi. L'impatto delle novità previste dal Regolamento per le pubbliche amministrazioni e i loro fornitori, tuttavia, appare ancora incerto. Alla luce delle nuove norme sul servizio di archiviazione elettronica, c'è il rischio che vengano compromesse le garanzie di certezza, qualità e affidabilità di documenti e archivi informatici delle pubbliche amministrazioni, che secondo la legge nazionale costituiscono beni culturali, patrimonio storico della nostra Repubblica. Occorre, dunque, un'attenta riflessione sulla possibilità e sull'opportunità di mantenere un regime speciale per le organizzazioni pubbliche.*

Abstract [EN]: *The eIDAS Regulation (EU Reg. No. 910/2014) establishes the European legal framework for the regulation of electronic trust services, including those related to the creation, management, and preservation of electronic documents. In the amending act to the Regulation (EU Reg. 2024/1183, known as "eIDAS 2.0"), there is a significant reduction in the current system of qualification for providers of such services, replaced by extensive referral through the implementing acts of the Regulation to supranational technical standards and norms. This should result in significant deregulation of the field and, at the same time, a substantial opening of the market for such services. However, the impact of the changes anticipated by the Regulation on public administrations and their suppliers remains uncertain. In light of the new rules on electronic archiving services, there is a risk that the guarantees of certainty, quality, and reliability of documents and electronic archives of public administrations, which according to national law constitute cultural assets and historical heritage of our Republic, may be compromised. Therefore, careful consideration is needed on the possibility and advisability of maintaining a special regime for public organizations.*

Parole chiave: eIDAS 2.0, gestione documentale, conservazione digitale, electronic archiving, CAD.

Sommario: 1. Il Regolamento eIDAS 2.0 e l'evoluzione della normativa europea in materia di trasformazione digitale. - 2. La gestione e conservazione dei documenti informatici nella normativa nazionale. - 3. eIDAS 2.0: dalla conservazione all'e-archiving. - 4. L'impatto di eiDAS 2.0 sulle politiche di gestione documentale del settore pubblico. - 5. Considerazioni conclusive.

1. Il Regolamento eIDAS e l'evoluzione della normativa europea in materia di trasformazione digitale

L'approvazione del Regolamento eIDAS 2.0[1] si inserisce nell'ambito di un ormai consolidato filone di norme eurounitarie che regolano, in modo sempre più stringente, il processo di trasformazione digitale della pubblica amministrazione italiana. Quello del rapporto tra ordinamento europeo e pubbliche amministrazioni è un tema particolarmente dibattuto nel recente dibattito scientifico[2].

Intatti, pure se non sono previste competenze specifiche delle istituzioni dell'Unione nella materia della digitalizzazione della pubblica amministrazione, in virtù del primato del diritto sovranazionale su quello nazionale (cfr. Corte Costituzionale n. 170 del 1984), le pubbliche amministrazioni applicano direttamente norme comunitarie in relazione all'uso delle tecnologie digitali. Si deve rilevare - e l'evoluzione del Regolamento eIDAS ne è l'evidente dimostrazione - che nel corso degli ultimi decenni abbiamo assistito ad un processo di espansione della normativa europea rilevante per le pubbliche amministrazioni, sia a causa dell'ampliamento delle materie di competenza delle istituzioni europee sia a causa dell'evoluzione del mercato unico quale spazio socio-economico.

Si tratta di un trend particolarmente evidente con riferimento alla digitalizzazione della pubblica amministrazione. Dal punto di vista normativo, l'intervento dell'UE nel settore della digitalizzazione trova il suo fondamento nella necessità di realizzare un "mercato unico digitale" efficiente e produttivo. Mentre nella prospettiva nazionale, la digitalizzazione delle pubbliche amministrazione risponde a obiettivi di efficienza, migliore allocazione delle risorse, incremento di efficacia dei

[1] Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 2014/910 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale, pubblicato in GU del 30 aprile 2024.

[2] Per una approfondita ricostruzione di questo dibattito si rinvia a S. Palumbo, *La transizione digitale della pubblica amministrazione italiana nella prospettiva europea. Considerazioni alla luce del Piano nazionale ripresa e resilienza*, in *Il diritto dell'economia*, 1, 2013.

servizi e garanzia dei diritti digitali, nella visione europea, l'amministrazione digitale è uno dei mezzi per la realizzazione del mercato unico europeo. È stato proprio in virtù della competenza sul mercato interno (art. 114 TFUE) che sono stati emanati alcuni dei più importanti provvedimenti europei in materia di innovazione digitale.

Sotto il profilo della tecnica della normazione, dopo una prima fase più rispettosa delle prerogative dei singoli Stati Membri, è prevalsa la tendenza all'adozione di atti direttamente vincolanti. A partire dai primi anni duemila, si è passati dalle direttive di armonizzazione alla moltiplicazione di strumenti regolamentari[3]. Il superamento del modello della direttiva è stato giustificato con la necessità di eliminare barriere al funzionamento del mercato interno, riducendo la frammentazione normativa - storicamente un ostacolo alle dinamiche concorrenziali - e contribuendo a raggiungere una maggiore certezza giuridica attraverso un insieme armonizzato di regole fondamentali che fanno ricorso a standard tecnologici comuni.

La necessità di regolamentare il mercato dei servizi IT in sede europea ha però risvolti significativi ben oltre il settore tecnologico, a causa della diffusione capillare delle tecnologie digitali in tutti gli ambiti istituzionali, economici e sociali della vita europea. Di conseguenza, le pubbliche amministrazioni si trovano a dover applicare[4] norme europee con riferimento all'identità digitale, alla protezione dei dati personali, alla cybersicurezza, all'accessibilità, alle firme e all'archiviazione elettronica.

2. La gestione e conservazione dei documenti informatici nella normativa nazionale

Il Regolamento UE 2024/1183 interviene in una materia in cui esiste una normativa nazionale assai stratificata in base alla quale le pubbliche amministrazioni esercitano le proprie attività istituzionali utilizzando gli strumenti ICT[5].

In particolare, per ottemperare all'obbligo di gestione informatica dei procedimenti, le amministrazioni devono ricorrere all'uso delle tecnologie informatiche in tutte le fasi delle procedure e, prioritariamente, nella formazione degli atti e

---

[3] Tra le principali si segnalano: il regolamento sulla protezione dei dati personali, il regolamento su servizi digitali, il regolamento eIDAS, il regolamento sui dati, il regolamento sulla governance dei dati, la proposta di regolamento sull'intelligenza artificiale.

[4] Sulla base dei principi elaborati dalle diverse corti costituzionali degli Stati Membri - ivi compresa la Corte italiana - le norme adottate dalle istituzioni unionali non possono però confliggere con - e quindi non possono prevalere su - i principi fondamentali e supremi dell'ordinamento costituzionale.

[5] Il primo principio guida del Piano triennale per l'informatica nella pubblica amministrazione (aggiornamento 2024-2026) è "digitale e mobile come prima opzione" (digital and mobile first) la cui definizione è '*Le pubbliche amministrazioni devono erogare i propri servizi pubblici in digitale e fruibili su dispositivi mobili, considerando alternative solo in via residuale e motivata, attraverso la "riorganizzazione strutturale e gestionale" dell'ente ed anche con una "costante semplificazione e reingegnerizzazione dei processi'*" (Rif. normativi: art.3-bis Legge n. 241/1990, art.1 c.1 lett. a) D. lgs. 165/2001, art.15 D. lgs. n. 82/2005, art.1 c.1 lett. b) Legge n. 124/2015, art.6 c.1 D. l. n. 80/2021).

nella gestione di archivi e comunicazioni[6]. Tali strumenti consentono di conferire all'attività compiuta con l'uso dell'informatica la stessa efficacia di quella compiuta tradizionalmente.

Infatti, in base alla normativa vigente:

- le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici;
- la protocollazione della comunicazioni in entrata e in uscita deve avvenire attraverso un sistema automatizzato;
- i fascicoli di procedimento sono informatici;
- le comunicazioni di documenti tra le pubbliche amministrazioni avvengono telematicamente;
- la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene telematicamente tutte le volte che il destinatario abbia un domicilio digitale;
- le pubbliche amministrazioni realizzano siti istituzionali attraverso i quali erogano i servizi on line e soddisfano gli obblighi di pubblicità legale.

In tale contesto, l'Italia, da decenni, ha introdotto un proprio quadro normativo organico al fine di consentire la gestione sicura di atti, documenti, comunicazioni e archivi nel proprio ordinamento, in modo da garantire certezza giuridica e fiducia nella transizione dalla modalità analogica a quella digitale.

La conservazione dei documenti informatici è stata regolamentata per la prima volta dalla Legge n. 537/1993, in base alla quale fu previsto che '*gli obblighi di conservazione e di esibizione dei documenti [...] si intendono soddisfatti anche se realizzati mediante supporto ottico purché le procedure utilizzate siano conformi a regole tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione*' (art. 2, comma 15).

Successivamente, il legislatore nazionale ha definito, adeguandolo alle norme progressivamente adottate in sede europea[7], un *corpus* organico di regole che ruotano intorno alle disposizioni del Testo Unico sulla Documentazione Amministrativa (D.p.r. n. 445/2000), del Codice dell'Amministrazione Digitale (D. lgs. n. 82/2005) e delle Linee guida adottate dall'Agenzia per l'Italia digitale in materia di formazione, gestione e conservazione dei documenti informatici[8].

Con riferimento specifico alla conservazione, l'art. 43, comma 1, D. lgs n. 82/2005 prevede che '*Gli obblighi di conservazione e di esibizione di documenti si*

---

[6] Per una ricostruzione puntuale degli obblighi normativi delle pubbliche amministrazioni italiane in materia di gestione documentale si rinvia a: E. Belisario, F. Ricciulli, S. Pagnotta, *Amministrazione Digitale*, Maggioli, 2021.

[7] Il legislatore nazionale ha provveduto prima all'adeguamento prima alla Direttiva 1999/93/CE e successivamente, in sede di riforma del Codice dell'Amministrazione digitale, alle modifiche necessarie a garantire la conformità alla prima versione del Regolamento eIDAS (Reg. UE 2014/910).

[8] L'ultima versione delle Linee guida Agid sul documento informatico è stata adottata, ai sensi dell'art. 71 D. lgs. n. 82/2005, con Determinazione n. 371 del 17 maggio 2021.

intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida.'. La normativa italiana dispone che, in tutti i casi in cui la legge prescrive obblighi di conservazione - anche a carico di soggetti privati - '*il sistema di conservazione dei documenti informatici assicura, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida*'. Vale la pena di rilevare che né il D.p.r. n. 445/2000 né il D. lgs. n. 82/2005 forniscono una definizione del termine 'conservazione' che, invece, è contenuta nel glossario delle Linee Guida Agid sul documento informatico (Allegato 1) come '*l'insieme delle attività finalizzate a definire e attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti*'.

3. eIDAS 2.0: dalla conservazione all'e-archiving

Il Reg. UE 2014/910, nella sua prima formulazione, si limitava a disciplinare lo strumento delle firme elettroniche per garantire autenticità e integrità dei documenti.

In fase di revisione, il legislatore europeo ha valutato l'opportunità di introdurre nel perimetro regolamentare anche il concetto di 'archiviazione elettronica' e il relativo servizio, proprio sulla scorta dell'esperienza di alcuni Stati Membri. tra cui l'Italia.

Infatti, si legge nel considerando 66 del Reg. UE 2024/1183:

'*Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione elettronica sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e documenti elettronici, nonché per i servizi fiduciari associati. Al fine di garantire la certezza giuridica, la fiducia e l'armonizzazione in tutti gli Stati membri, è opportuno istituire un quadro giuridico per i servizi di archiviazione elettronica qualificati, ispirato al quadro per gli altri servizi fiduciari di cui al presente regolamento. Il quadro giuridico per i servizi di archiviazione elettronica qualificati dovrebbe offrire ai prestatori di servizi fiduciari e agli utenti un pacchetto di strumenti efficiente che comprenda requisiti funzionali per il servizio di archiviazione elettronica, nonché chiari effetti giuridici in caso di utilizzo di un servizio di archiviazione elettronica qualificato. Tali disposizioni dovrebbero applicarsi ai dati elettronici e ai documenti elettronici creati in forma elettronica e ai documenti cartacei che sono stati scannerizzati e digitalizzati. Ove necessario, tali disposizioni dovrebbero consentire che i dati elettronici e i documenti elettronici conservati siano trasferiti su supporti o formati diversi al fine di estenderne la durabilità e la leggibilità oltre il periodo di validità tecnologica,*

evitando nel contempo, nella misura del possibile, le perdite e le alterazioni.'.

All'interno delle definizioni di eIDAS, quindi, entra anche quella di *e-archiving*, archiviazione elettronica, concepita come '*un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione*' (art. 3, n. 48, Reg. UE 2014/910).

A prescindere dal ricorso all'uso del termine 'conservazione', è di palmare evidenza che gli obiettivi che il servizio di archiviazione elettronica - non qualificato o qualificato[9] - deve raggiungere siano del tutto analoghi a quelli che il legislatore nazionale ha affidato ai sistemi di gestione e conservazione documentale: leggibilità, certezza giuridica, reperibilità dei documenti, integrità, sicurezza, affidabilità, autenticità, mantenimento del valore probatorio.

È ugualmente importante esaminare le implicazioni giuridiche dell›archiviazione elettronica come stabilite dall›articolo 45 decies del Regolamento eIDAS così come recentemente modificato.

In particolare, sono disciplinati:

- servizio di archiviazione elettronica non qualificato: ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.
- servizio di archiviazione elettronica qualificato: i dati elettronici e i documenti elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della presunzione della loro integrità e della correttezza della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato.

Con specifico riferimento ai requisiti per i servizi di archiviazione elettronica qualificati, l'art. 45 undecies Reg. UE 2014/910, introdotto nella modifica che si commenta, dispone che

a. sono forniti da prestatori di servizi fiduciari qualificati;
b. utilizzano procedure e tecnologie in grado di garantire la durabilità e la leggibilità dei dati elettronici oltre il periodo di validità tecnologica e almeno per tutto il periodo di conservazione legale o contrattuale, preservandone nel contempo l'integrità e l'esattezza dell'origine;
c. assicurano che i dati elettronici siano conservati in modo tale da essere

[9] Ai sensi dell'art. 3, n. 49, Reg. UE 2014/910 per 'servizio di archiviazione elettronica qualificato' si intende ' un servizio di archiviazione elettronica fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 undecies'.

protetti dal rischio di perdita e alterazione, ad eccezione delle modifiche riguardanti il loro supporto o il loro formato elettronico;

d. consentono alle parti autorizzate facenti affidamento sulla certificazione di ricevere una relazione in un modo automatizzato in cui si conferma che i dati elettronici consultati da un archivio elettronico qualificato godono della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento della consultazione; tale relazione è fornita in modo affidabile ed efficiente e reca la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore del servizio di archiviazione elettronica qualificato.

Infine, il Regolamento prevede che entro il 2025 la Commissione europea - mediante atti di esecuzione - stabilisca norme e procedure specifiche per i servizi di archiviazione elettronica qualificati, che se rispettate, confermano il rispetto dei requisiti richiesti. Questa misura è volta a standardizzare ulteriormente le prassi di conservazione digitale e a rafforzare la fiducia nel sistema europeo di archiviazione elettronica.

4. L'impatto di eiDAS 2.0 sulle politiche di gestione documentale del settore pubblico

Sebbene l'attenzione di molti commentatori si sia inizialmente appuntata su altri profili di eIDAS 2.0 (come l'EUDI wallet), l'introduzione della disciplina dei servizi di *e-archiving* rappresenta una delle principali novità del Reg. UE 2024/1183, in quanto - specialmente nel nostro Paese, alla luce della disciplina sulla conservazione di cui al § 2 del presente contributo - è destinata a produrre cambiamenti rilevanti sia per i fornitori di servizi che per le pubbliche amministrazioni.

Nonostante alcune difficoltà iniziali, il modello adottato finora in Italia ha contribuito a sensibilizzare il settore pubblico riguardo le sfide e le complessità del mantenere nel tempo le memorie digitali[10] e ha, al tempo stesso, creato un mercato di fornitori di servizi di conservazione iscritti in un marketplace tenuto dall'Agenzia per l'Italia Digitale[11].

---

[10] In questo senso M. Guercio, *Nuovo eIDAS, le proposte per archiviazione e conservazione: verso più controllo*, in *Agenda Digitale*, 19 settembre 2023 (raggiungibile all'Url https://www.agendadigitale.eu/documenti/nuovo-eidas-le-proposte-per-archiviazione-e-conservazione-verso-piu-controllo/).

[11] L'art. 34, comma 1-bis, D. lgs. n. 82/2005 prevede che le pubbliche amministrazioni possano procedere alla conservazione dei documenti informatici con una delle seguenti modalità:
a) all'interno della propria struttura organizzativa;
b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione

Con eIDAS 2.0 si delinea inevitabilmente un nuovo panorama competitivo. L'art. 24-bis del Reg. UE 2014/910, così come modificato, prevede che '*un servizio di archiviazione elettronica qualificato fornito in uno Stato membro è riconosciuto quale servizio di archiviazione elettronica qualificato in tutti gli altri Stati membri*'. L'introduzione del mutuo riconoscimento dei servizi di conservazione tra gli Stati membri crea un effetto simile a quello già ottenuto per le firme qualificate, eliminando le barriere tra i Paesi e creando un unico mercato europeo anche per l'*e-archiving*. Si tratta di un mutamento significativo che rappresenta sia un'opportunità per operatori di mercato che possono vantare una indubbia esperienza nel campo dell'archiviazione digitale sia un rischio, legato all'arrivo di nuovi *competitor* sul mercato italiano e al tempestivo aggiornamento di regole di qualificazione, rispettose degli atti di esecuzione previsti dall'art. 45-undecies Reg. UE 2014/910, in modo da evitare ingiustificate disparità di trattamento con gli altri operatori europei.

Inoltre, a fronte delle norme dettate in sede europea per la creazione di un mercato unico dei servizi di conservazione, bisogna investigare quale sia il residuo margine di regolazione rimesso ai legislatori nazionali in materia di conservazione. È lo stesso Reg. UE 2024/1183 ad aprire a una riserva di normazione per i singoli Stati membri con il Considerando n. 66 in base al quale '*Le attività degli archivi nazionali e delle istituzioni della memoria, in qualità di organizzazioni preposte alla conservazione del patrimonio documentario nell'interesse pubblico, sono generalmente disciplinate dal diritto nazionale e non forniscono necessariamente servizi fiduciari ai sensi del presente regolamento.*'.

Inoltre, giova ricordare quanto riportato nell'introduzione al presente contributo in ordine al fatto che le norme eurounitarie non possono prevalere sui principi fondamentali dei rispettivi ordinamenti costituzionali. In proposito, va rilevato che - tra i principi fondamentali della Carta Costituzionale - l'art. 9 espressamente prevede che la Repubblica '*tutela il paesaggio e il patrimonio storico e artistico della Nazione.*'. In attuazione di questa disposizione costituzionale, il legislatore ha adottato il D. lgs. n. 42/2004 (Codice dei beni culturali e del paesaggio)[12] che all'art. 10, comma 2, lett. b), espressamente include tra i beni culturali '*gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico*'.

e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

[12] L'art. 1, D. lgs. n. 42/2004 recita:
'*1. In attuazione dell'articolo 9 della Costituzione, la Repubblica tutela e valorizza il patrimonio culturale in coerenza con le attribuzioni di cui all'articolo 117 della Costituzione e secondo le disposizioni del presente codice.*
2. La tutela e la valorizzazione del patrimonio culturale concorrono a preservare la memoria della comunità nazionale e del suo territorio e a promuovere lo sviluppo della cultura.
3. Lo Stato, le regioni, le città metropolitane, le province e i comuni assicurano e sostengono la conservazione del patrimonio culturale e ne favoriscono la pubblica fruizione e la valorizzazione.'

Apparentemente, quindi, residua un margine di disciplina in capo al legislatore nazionale e, quindi, dal punto di vista tecnico all'Agenzia per l'Italia digitale, ma solo per quanto riguarda le amministrazioni (così come definite dall'art. 1, comma 2, D. lgs. n. 82/2005) e nei limiti in cui i rispettivi documenti e dati possano rientrare nella definizione di archivio precedentemente fornita.

Questo potrebbe comportare indubbiamente una rilevante novità per il nostro ordinamento: la differenziazione tra la normativa applicabile alla conservazione dei dati e dei documenti dei privati (Reg. eIDAS così come recentemente modificato) e la normativa applicabile agli archivi delle amministrazioni (attraverso una novella del Codice dell'Amministrazione Digitale).

Fin qui, infatti, le norme sull'efficacia giuridica e probatoria dei documenti sono state le medesime, con alcune differenze dovute ai peculiari obblighi di conservazione di determinati atti e documenti incombenti sulle pubbliche amministrazioni.

Infatti, la versione vigente del'art. 2, comma 3, del Codice dell'Amministrazione Digitale espressamente prevede che "*Le disposizioni del presente Codice e le relative Linee guida concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto.*".

Pertanto, nell'ambito del necessario intervento di modifica alla normativa nazionale, il legislatore sarà chiamato a valutare sulla possibilità e opportunità di mantenere un regime speciale per le organizzazioni pubbliche ulteriore rispetto alla previsione dell'obbligo per le amministrazioni di ricorrere a servizi di archiviazione elettronica qualificati di cui all'art. 45 undecies Reg. UE 2014/910. Tali modifiche dovranno essere valutate ponderando con attenzione la necessità di restringere la concorrenza e, di conseguenza, il numero degli operatori che potranno fornire servizi di conservazione alle pubbliche amministrazioni italiane.

5. Considerazioni conclusive

Il panorama della gestione documentale nelle pubbliche amministrazioni è destinato a subire una significativa evoluzione dopo la pubblicazione del Regolamento eIDAS 2.0. Questa modifica normativa, che si propone di armonizzare e potenziare i servizi digitali a livello europeo, anche attraverso atti nazionali di adeguamento, inciderà sulle modalità con cui le amministrazioni operano.

Indubbiamente, l'introduzione nel Regolamento eIDAS 2.0 dei servizi di archiviazione elettronica rappresenta un riconoscimento significativo per l'elaborazione normativa e alcune pratiche nazionali in materia di conservazione dei documenti digitali. Si tratta di un cambiamento che riconosce l'insufficienza della firma per garantire l'integrità e l'autenticità dei documenti digitali a lungo termine. Tuttavia,

se è vero che l'esperienza italiana può avere ispirato la norma europea, è altrettanto indiscutibile che il punto di approdo del legislatore sovranazionale non sia quello italiano.

A tal proposito, fatte salve poche e lodevoli eccezioni, sorprende la scarsità di dibattito sull'impatto delle nuove regole europee sulle norme che disciplinano le prassi amministrative degli enti pubblici in materia di conservazione. Infatti, come sopra evidenziato, tanto il Codice dell'Amministrazione Digitale quanto le relative Linee guida sulla conservazione dovranno essere adattate per conformarsi ai nuovi standard europei.

I punti oggetto di attenzione per futuro adeguamento normativo dovranno essere:

- il riconoscimento del ruolo che nella normativa sovranazionale assumono i "dati" ai quali il CAD e le Linee guida attuali riservano attenzione secondaria rispetto ai "documenti";
- la differenziazione delle disposizioni applicabili agli archivi delle amministrazioni rispetto a quelli privati.

Tali modifiche normative, benché limitate dal ristretto margine di manovra lasciato ai legislatori nazionali, dovranno essere attentamente ponderate per evitare conflitti con le norme comunitarie e per consentire alle amministrazioni pubbliche e al mercato di sfruttare appieno il vantaggio conferito dall'esperienza pregressa. È quindi cruciale che le future norme siano chiare e tempestive, non solo per rispettare le disposizioni europee, ma anche per facilitare l'adeguamento e l'ottimizzazione dei sistemi esistenti.

In questo scenario, la definizione di indicazioni chiare per il *procurement* e l'aggiornamento dei sistemi diventerà un aspetto cruciale anche per le azioni da inserire nel Piano triennale per l'informatica nella pubblica amministrazione.

In conclusione, quindi, la pubblicazione in Gazzetta Ufficiale del Reg. UE 2024/1183 rende urgente l'avvio di un percorso partecipato che porti alla novellazione del CAD e delle Linee Guida per prevenire contrasti tra la normativa comunitaria e quella nazionale, collaborando al tempo stesso con gli enti di standardizzazione per la redazione di norme tecniche che tengano conto dell'esperienza e delle garanzie fin qui assicurate dai sistemi di conservazione.

N. 4 - 2024 - pp. 42-53

L'evoluzione del documento informatico nel nuovo quadro giuridico dell'eIDAS 2

Andrea Lisi

Abstract [IT]: L'evoluzione concettuale del documento non può ritenersi correlata solo agli aspetti definitori, ma va inquadrata nel contesto dei servizi fiduciari che, modificandosi, garantiscono nuove possibilità di sviluppo interpretativo per le rappresentazioni digitali di fatti, atti o dati giuridicamente rilevanti. E se, in passato, la "conservazione digitale" poteva essere considerata come termine generico che inquadrasse diverse fattispecie di consolidamento di un contenuto digitale giuridicamente rilevante. Adesso la conservazione può (e forse deve) riferirsi all'archiving, offrendo prospettive diverse nell'interpretazione delle forme documentali digitali che si svilupperanno nel prossimo futuro.

Abstract [EN]: The conceptual evolution of the document cannot be considered to be related only to definitional aspects, but must be framed in the context of trust services, which, as they change, guarantee new possibilities of interpretative development for digital representations of legally relevant facts, acts or data. And if, in the past, "digital preservation" could be considered as a generic term framing various cases of consolidation of legally relevant digital content. Now preservation can (and perhaps must) refer to archiving, offering different perspectives in the interpretation of digital documentary forms that will develop in the near future.

Parole chiave: Documento informatico, digitalizzazione, archiving, conservazione.

Sommario: 1. Premesse. La metamorfosi del documento informatico - 2. Dalla res signata alla vertigine della forma digitale affidabile - 3. L'esigenza di documentare - 4. Definizioni: l'evoluzione concettuale del nuovo eIDAS - 5. Conclusioni: il documento informatico a formazione progressiva in Italia e in Europa

1. Premesse. La metamorfosi del documento informatico

Mai come oggi si sta compiendo una radicale metamorfosi del documento lungo i tempi scanditi dagli algoritmi dei sistemi delle intelligenze artificiali generative.

"Un mattino, al risveglio da sogni inquieti, Gregor Samsa si trovò trasformato

in un enorme insetto. Sdraiato nel letto sulla schiena dura come una corazza, bastava che alzasse un po' la testa per vedersi il ventre convesso, bruniccio, spartito da solchi arcuati; in cima al ventre la coperta, sul punto di scivolare per terra, si reggeva a malapena. Davanti agli occhi gli si agitavano le gambe, molto più numerose di prima, ma di una sottigliezza desolante". Il racconto La metamorfosi di Franz Kafka[1] non può non farci annusare metaforicamente il cambiamento radicale che sta vivendo oggi l'arte di documentare.

Nella frenesia del mondo del social web ciò che si documenta sfugge sempre di più all'archivio[2], sia in ambito strettamente giuridico o amministrativo, sia in altri ambiti come quello letterario, musicale o cinematografico, dove tutti i contenuti sono ormai digitali e spesso vengono condivisi trasversalmente in diversi ambienti che solo in apparenza "ci appartengono", sottraendone la diffusione al controllo dei singoli autori. Tutto viene partecipato, contaminato, dato in pasto ad algoritmi, diffuso nella miriade dei bit perdendo il senso del contesto e dell'affidabilità delle fonti di pubblicazione. Tutto è reso disponibile ovunque, ma l'ovunque ubiquo è indeterminato e indeterminabile e spesso (e incredibilmente) favorisce la dispersione del documento nelle sue certezze derivanti dall'origine della sua produzione.

Il dato informativo quindi c'è ancora, anzi c'è troppo, perché nella sua dissennata contaminazione ha lasciato per strada la certezza giuridica e il contesto archivistico. E quindi non è più garantito nella sua autenticità.

È indubbio, infatti, che si stia assistendo in questi ultimi anni a una crisi informativa generata da un aumento esponenziale e disordinatissimo di dati e informazioni non documentate. I sistemi di intelligenza artificiale e di generazione di notizie (prima affidate a fonti autorevoli e verificabili) oggi, scandagliando minuziosamente il web, ci regalano sintesi inesatte, assiomi indimostrabili, presunzioni di "verità", spesso indirizzate a noi in modo ben impacchettato secondo nostri gusti e abitudini di navigazione (perché siamo stati previamente profilati). Sostanzialmente vengono rafforzate nostre convinzioni, cancellando del tutto la capacità di critica che è fondata sulla verifica e, quindi, sulla ricerca di fonti documentali.

Il Regolamento UE eIDAS 2[3], come vedremo nel presente contributo, potrebbe

---

[1] La metamorfosi (Die Verwandlung in tedesco) è il racconto più noto dello scrittore boemo Franz Kafka. L'opera fu pubblicata per la prima volta nel 1915 dal suo editore Kurt Wolff a Lipsia.

[2] *Nel caso degli archivi digitali l'evoluzione ha riguardato di volta in volta il sistema operativo, gli applicativi, i supporti di archiviazione, i dispositivi di scrittura. Preservare a lungo termine le memorie collettive e personali degli ultimi decenni è un'impresa resa particolarmente complessa dalla necessità di integrare competenze appartenenti ad ambiti considerevolmente diversi: discipline letterarie, tecniche archivistiche, tecnologia dell'informazione, questioni giuridiche, aspetti amministrativi. Inoltre, la gestione dell'archivio digitale presuppone l'aggiornamento costante dei modelli di dati, degli standard e delle procedure per far fronte alla crescente varietà delle fonti documentarie*, così Paul Gabriele Weston, Emmanuela Carbè, Primo Baldini in Se i bit non bastano: pratiche di conservazione del contesto di origine per gli archivi letterari nativi digitali. Il pdf è scaricabile direttamente dal sito della Rivista open access Bibliothecae.it – ISSN 2283-9364: https://bibliothecae.unibo.it/index.

[3] Si fa riferimento ovviamente al Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione

costituire un fondamentale argine a tutto questo, molto più rilevante – almeno dal punto di vista documentale - rispetto al più imprevedibile e incerto AI Act[4], il quale si occupa di altri aspetti della materia digitale e dei suoi rischi di impatto per i diritti e libertà fondamentali che ci riguardano. Infatti, in eIDAS 2 finalmente ci si occupa (e ci si preoccupa) di "e-archiving", di registrazioni affidabili, di documenti in grado di salvaguardare la nostra memoria digitale, preservando la fonte di provenienza. E, in un mondo ormai tristemente caratterizzato dalla diffusione sistematica di deep fake e fake news - un mondo dove ormai i siti web degli anni '90 sono già "storia" da dimenticare e, infatti, il motore di ricerca Google ha scelto tranquillamente di disinteressarsene e non li raccoglieremo più nelle nostre dissennate ricerche affidate agli algoritmi profilatissimi (e mai casuali) che ci riguardano - questa attenzione alle regole dell'archiviazione elettronica finisce per essere un'attività rivoluzionaria. Fino a oggi purtroppo la memoria del web rimane affidata alle follie desuete di strani progetti che inseguono ciò che non ci interessa più, la storia di noi, di soli pochi anni fa. Progetti come Archive.org, Oldwebtoday o Web Design Museum[5].

Ci rimane pertanto una speranza: recuperare il senso del ricordo affidabile. Ci rimangono il Digital Archiving di eIDAS 2 e il recupero di competenze strategiche per un futuro digitale che continui a poggiarsi affidabilmente sulla Storia (e quindi sui presupposti solidi delle nostre democrazie).

2. Dalla res signata alla vertigine della forma digitale affidabile

Anni fa, ragionando sui nuovi scenari del documento informatico, ci si chiedeva provocatoriamente se il documento informatico fosse in grado di documentare con caratteristiche parificabili alla forma scritta analogica[6]. E si rifletteva sul fatto che probabilmente non avesse più alcun senso utilizzare ancora il termine "forma scritta" per il contesto digitale sostituendola, ad esempio, con "forma digitale affidabile"[7],

del quadro europeo relativo a un'identità digitale.

[4] Si fa riferimento al Regolamento europeo che stabilirà delle regole armonizzate sull'intelligenza artificiale e andrà a modificare i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale).

[5] Così Luca Tremolada, La fine dei siti web è iniziata prestissimo, Nova, Sole24Ore, 21 aprile 2024, N. 110, pag. 16.

[6] In Editoriale: La "metamorfosi" del documento informatico, in KnowIT. Periodico trimestrale. Anno II N. 2 - Luglio 2017 - ISSN 2532-1684. Qui reperibile: https://studiolegalelisi.it/wp-content/uploads/2017/07/KnowIT_Luglio_2017.pdf

[7] *C'è davvero oggi differenza sostanziale tra un Registro IVA o un Libro Giornale che contengono i dati contabili aggiornati dell'impresa oppure un Registro di protocollo informatico di una PA o un Registro di Log di un portale di e-commerce dal quale si evincono i dati aggiornati e profilati sui gusti e le abitudini dei clienti on line? Ormai si tratta sempre e solo di registrazioni indipendenti*

ponendosi così alcune domande che si ritenevano fondamentali al fine di interrogarsi sulle nuove evoluzioni documentali e sul "vero" documento nativo digitale. In particolare, ci si domandava:

- È realmente considerabile documento nativo digitale il documento redatto in un formato "testo" in modo da poter essere utilizzato in modo simile al documento cartaceo, oppure più propriamente il formato strutturato registrato in modo affidabile che preservi le correlazioni del testo che contiene?
- Il futuro della conservazione della memoria digitale sarà affidato a precisi formati documentali custoditi in modo (più o meno) tradizionale o sempre di più a metadati dinamici contenenti i campi essenziali (es. stringhe di caratteri, sia per i valori dei campi sia per i loro descrittori che sarebbero in grado di ricostruire dinamicamente il layout del documento in ogni momento) da registrare in modo affidabile nel tempo attraverso custodie ininterrotte a livello informatico?
- E l'autenticità, quindi, nei contesti digitali si può perseguire ancora con un'attenzione alla forma documentale o invece ci si deve necessariamente concentrare sulle registrazioni attendibili di contenuti rilevanti sviluppate e garantite sin dalla loro origine da soggetti affidabili?

Sono domande che non hanno perso la loro attualità, pur se nel loro senso compiuto appaiono pericolosamente superate in un'evoluzione forsennata verso le intelligenze artificiali generative che, attraverso sofisticati algoritmi di apprendimento, acquisiscono miliardi di informazioni contenuti negli sterminati database del web e regalano mirabili sintesi. Ma le troppe informazioni di cui si dispone oggi finiscono per (paradossalmente) disinformare, se non sono ben incastonate in un archivio digitale.

Per tale motivo, è necessario recuperare concettualmente il senso di documentare nel mondo delle intelligenze artificiali di cui tanto si discute in questi giorni.

3. L'esigenza di documentare

È possibile affermare che la capacità – o meglio – la necessità di documentare, ossia di lasciare "una traccia" materiale e affidabile del proprio passaggio e degli eventi maggiormente rappresentativi a esso legati, sia sempre stata parte della natura umana[8]. Basti pensare che la fine stessa della Preistoria – e l'inizio della Storia – è

da supporti e sempre più leggibili in modo "mediato", rese disponibili e autentiche attraverso l'opera di intermediari responsabili, così in Editoriale: La "metamorfosi" del documento informatico, in KnowIT, *cit*.

[8] Così Francesca Cafiero e Andrea Lisi, Dal segnare al consegnare: la formazione progressiva del documento all'interno del contesto (archivistico) digitale, in KnowIT. Periodico trimestrale. Anno

convenzionalmente scandita dall'incredibile "invenzione" della scrittura. La scrittura è, infatti, considerata un elemento fondamentale di tutte le grandi civiltà, a eccezione di quella degli Incas del Perù, i quali non la conoscevano, pur affidandosi ad altri strumenti per garantire la documentazione delle proprie azioni [9].

Tuttavia, la facoltà di documentare, intesa come la capacità di porre in essere una «res rappresentativa di un fatto»[10], risponde a un'esigenza di natura più complessa e meno immediata, che ha subìto un iter evolutivo ben preciso nel corso dei secoli. Per comprendere e conoscere appieno la genesi e le forme che caratterizzano l'oggetto documentale è necessario adottare infatti l'approccio critico fornito dalla diplomatica generale, la scienza nata per studiarne le caratteristiche intrinseche ed estrinseche, così come i fattori che concorrono nel contesto di produzione[11].

Ebbene, dal punto di vista simbolico è proprio il gesto fisico e personalissimo di apporre un segno attestante la propria identità a essersi accompagnato per secoli all'esigenza di documentare, anche quando si trattava di tracciare solo una semplice croce la quale, per quanto anonima, attestava comunque un legame biometrico indissolubile con la res signata e, per quanto superflua ai fini del perfezionamento dell'atto, testimoniava a tutti gli effetti una partecipazione attiva al confezionamento dello stesso. In effetti, nel mondo non digitale le sottoscrizioni delle parti non risultano sempre indispensabili qualora la testimonianza formale venga perfezionata in presenza di un pubblico ufficiale. Ciò consente, ad esempio, di formalizzare l'atto

I N. 1 - Dicembre 2016, qui reperibile: https://studiolegalelisi.it/wp-content/uploads/2016/12/KnowIt_Dicembre_2016.pdf

[9] Essi avevano, infatti, un altro medium per conservare le informazioni. Si tratta del quipu, una serie di corde di diversa lunghezza, spessore e colore intrecciate tra di loro. Info: http://www.lacomunicazione.it/voce/storia-della-comunicazione/, 2016

[10] Dal punto di vista strettamente giuridico, come è noto, la definizione di documento quale res rappresentativa di un fatto appartiene a Francesco Carnelutti, Teoria Moderna, In Novissimo Digesto Italiano, 1975. Non può non ricordarsi anche la definizione di res signata di Natalino Irti, 1969.

[11] *Anzitutto occorre considerare la dimensione spazio-temporale del documento, la cui stesura segue solitamente l'actio, ossia l'azione di carattere giuridico, posta in essere da un autore e indirizzata generalmente a un destinatario, il cui ruolo passivo è necessario ai fini propri dell'esecutività. Storicamente e per gli atti di maggior rilievo, tra questi due soggetti può intercorrere fisicamente e temporalmente un terzo attore: l'estensore materiale dell'oggetto documentale che ne qualifica l'autenticità, il pubblico ufficiale. Le origini della sua professionalità risalgono all'epoca medievale, quando al documento veniva riconosciuta, appunto, una validità di tipo giuridico solo quando confezionato per conto di un'autorità pubblica (publica auctoritas) o comunque redatto da una figura solenne (scrittore o "rogatario"). L'azione di questo mediatore era circoscritta nell'ambito di una fase ben precisa, la conscriptio, ossia la stesura del documento per conto degli attori protagonisti dell'actio, la cui memoria era così definitivamente attestata e garantita nel tempo sul piano probatorio. Il perfezionamento della res documentale avveniva poi grazie «all'osservanza di certe determinate forme, […] destinate a procurarle fede e a dare forza di prova»* [definizione di Cesare Paoli (1840-1902)] *ossia di determinate formalità, sul piano sia intrinseco che estrinseco, tra le quali si annoveravano altresì le sottoscrizioni (in ambito privatistico, spesso signum crucis, segni di croce) apposte nella parte finale, definita "escatocollo",* così Francesca Cafiero e Andrea Lisi, Dal segnare al consegnare: la formazione progressiva del documento all'interno del contesto (archivistico) digitale, in KnowIT, cit..

pubblico anche con il "croce-segno" dell'analfabeta[12].

Fino a pochi anni fa anche le tecnologie introdotte in ambito documentale hanno provato a inseguire in punto di diritto un impossibile parallelismo tra il documento cartaceo, sottoscritto con firma autografa, e il documento informatico, sottoscritto per mezzo della firma digitale.[13] Tale esigenza formale può trovare ancora riscontro nel diritto positivo, ma è possibile riferire che sia stato ampiamente superato il dualismo firma digitale/firma autografa a garanzia della formazione di scritture private e documenti garantiti dalla "forma scritta": anzi, la forma scritta digitale (ad probationem o ad substantiam che sia) può oggi prescindere dalle stesse firme elettroniche legate al documento informatico (le quali possono limitarsi a qualificarne l'imputabilità giuridica), perché va appunto considerata un'"attitudine" dello stesso – nei suoi tanti formati e caratteristiche dinamiche – a documentare. Infatti, il Codice dell'amministrazione digitale (in seguito CAD)[14], nell'art. 20, comma 1-bis, riconosce l'idoneità del documento informatico a soddisfare il requisito della forma scritta prescindendo dalla sussistenza di una firma elettronica collegata allo stesso e riconduce il suo valore probatorio alla valutazione delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità[15].

Si è ormai, nel nostro ordinamento nazionale, passati da una concezione più tradizionale della formazione del documento prodotto attraverso un software di word processor o attraverso un'acquisizione della sua immagine via scanner a una visione più moderna e dinamica di documento, individuabile come una registrazione durevole di flussi informativi giuridicamente rilevanti[16]. La stessa locuzione latina *verba volant scripta manent* andrebbe riadattata e rimodellata in base ai nuovi

---

[12] Di contro – sempre secondo il codice civile italiano – il documento formato da ufficiale pubblico incompetente o incapace ovvero senza l'osservanza delle formalità prescritte, se è stato sottoscritto dalle parti, ha la stessa efficacia probatoria della scrittura privata.

[13] Si fa riferimento ovviamente al Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 – Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59.

[14] Si fa riferimento al (più volte rivisitato) Decreto Legislativo 7 marzo 2005, n. 82.

[15] In realtà,il Legislatore è giunto a promuovere il superamento della corporeità della sottoscrizione, nell'evoluzione giuridica e diplomatistica del documento, permettendo addirittura di prescindere dall'utilizzo diretto di firme elettroniche in senso stretto nei modelli di transazione dell'e-commerce e dell'e-government. In realtà, già in ambito privatistico, l'e-commerce aveva avvertito per primo, fin dai suoi albori, l'esigenza di sradicarsi dai meccanismi del formalismo documentale, in favore di regimi che permettessero contrattazioni transfrontaliere basate su documenti dichiarativi non sottoscritti, ma comunque in grado di attestare con certezza la paternità dell'azione dal punto di vista giuridico. Ne scrivevo già nel 2004, in La crisi d'identità del documento informatico: riflessioni sulla forma scritta, "firmata" non sottoscritta nel commercio elettronico internazionale, su Jei – Jus e Internet, 18 Marzo 2004, acquisibile qui: https://www.jei.it/approfondimenti-giuridici/281-la-crisi-d-identita-del-documento-informatico-riflessioni-sulla-forma-scritta-firmata-non-sottoscritta-nel-commercio-elettronico-internazionale.

[16] Così, Andrea Lisi, La custodia affidabile del documento informatico nell'era delle nuvole, in Revista de Ciencia de la Legislación - Número 10 - Septiembre 2021, IJ-I-DCCCXCIV-458. Raggiungibile a questo link: https://ar.ijeditores.com/pop.php?option=articulo&Hash=03b7c4073e0979787df3312748ef5509.

strumenti di comunicazione multicanale di cui dispone oggi la società digitale e con essi si deve fare i conti, ripensando allo stesso ruolo di terze parti fidate che possano cooperare con i contraenti/soggetti che manifestano le loro volontà in ambienti digitali riservati all'interlocuzione on line affidabile, garantendo così a tali manifestazioni di volontà espresse in modo diverso (sotto forma essenzialmente di file di log giuridicamente rilevanti) una staticizzazione e una conservazione in forma digitale autentica.

L'imputabilità della volontà contrattuale trasfusa nel documento informatico, nondimeno, è oggi determinabile – nell'e-commerce, come nell'e-gov – attraverso tecniche di autenticazione (*rectius* identificazione informatica o - meglio ancora - verifiche della nostra identità digitale), legate non tanto al documento inteso come res signata, ma alla sua formazione, o meglio al controllo dei processi propedeutici alla formazione dell'atto che può contenere una firma elettronica. La "vecchia" res, che garantiva l'esigenza di corretta documentazione nella definizione carneluttiana, viene oggi ritrovata e sostituita dalla corretta e integra registrazione informatica dell'atto giuridicamente rilevante secondo determinate procedure, conformi a regole tecniche condivise a livello nazionale, che ne qualifichino, appunto, l'affidabilità.

Se "prima" i documenti cartacei per determinate garanzie formali dovevano essere firmati e sottoscritti, ora i documenti informatici sono formati e trasmessi attraverso partner fidati come previsto da tempo proprio dal Regolamento eIDAS che si occupa, come ben sappiamo, di identificazione elettronica e servizi fiduciari[17]. Viene sancito, dunque, un'ulteriore evoluzione, un passaggio fondamentale: dal "segnare" al "consegnare" un documento (informatico). Il partner fidato, che garantisce certi processi informatici o eroga "servizi fiduciari" è il soggetto che – previa verifica di affidabilità da parte delle autorità competenti, nel caso in cui siano soggetti "qualificati" – concorre alla formazione, gestione, firma, trasmissione, oggi anche conservazione dei documenti informatici. Proprio in questa prospettiva, in effetti, le firme elettroniche "non firmano" (o meglio non sottoscrivono), ossia non sono apposte "sul documento" per attribuirne l'imputabilità giuridica, bensì sono associate a quel contenuto giuridicamente rilevante, "validando" processi digitali: esse, cioè, attribuiscono quel contenuto – con un diverso valore giuridico e probatorio in base alla sicurezza e all'affidabilità del processo – a un determinato soggetto dell'ordinamento.

[17] Così, Francesca Cafiero e Andrea Lisi, Dal codice alle linee guida: Il percorso della digitalizzazione documentale in Italia, in Revista de Ciencia de la Legislación - Número 12 - Octubre 2022, IJ-III-DLXVI-153. Raggiungibile a questo indirizzo: https://ar.ijeditores.com/pop.php?option=articulo&Hash=68c1f4a2f4755ddc850abd8577b300f4.

4. Definizioni: l'evoluzione concettuale del nuovo eIDAS

Tale evoluzione concettuale del senso stesso di documentare nel mondo digitale trova un suo fondamento oggi nell'ordinamento europeo. Negli ultimi regolamenti UE dedicati alla digitalizzazione che riguarda mercati e pubbliche amministrazioni i dati vengono definiti come "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva"[18].

Tale definizione di dato si avvicina concettualmente all'attuale definizione di documento informatico presente nel nostro ordinamento. Nel Codice dell'amministrazione digitale, infatti, ritroviamo la seguente definizione di documento informatico: "documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1, comma 1, lett. p)) che si contrappone a quella di documento analogico, definito semplicemente come documento non informatico (art. 1, comma 1, lett. p-bis)). E, secondo l'art. 3 del Regolamento eIDAS, il documento elettronico è qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva[19]. Il regolamento eIDAS, quindi, completa la definizione di documento informatico contenuta nel CAD[20]. Inoltre, non si può non ricordare, ai nostri fini, anche l'art. 22 della legge 7 agosto 1990, n. 241 (contenente le nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi), secondo il quale deve intendersi per documento amministrativo "ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e

[18] Si fa riferimento al Regolamento UE 2022/868 del 30 maggio 2022 (art. 2 par. 1 punto 1) relativo alla governance europeo dei dati e al Regolamento UE 2023/2854 del 13 dicembre 2023 (art 2 par. 1 punto 1) riguardante norme armonizzate sull'accesso equo ai dati e al loro utilizzo.

[19] In base all'art. 20 del CAD, il documento informatico soddisfa il requisito della forma scritta (acquisendo anche il valore probatorio di cui all'art. 2702 Cod. civ., ossia della scrittura privata) quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. La formulazione dell'art. 20 del CAD, comunque, ricomprende la validità giuridica anche per il documento informatico che in generale rispecchi i requisiti di sicurezza, integrità e immodificabilità e a cui sia apposta una qualunque firma elettronica, anche una firma elettronica "semplice" (purché, appunto, la riconducibilità all'autore sia "manifesta e inequivoca").

[20] Le disposizioni contenute nell'art. 20 del CAD risultano, pertanto, in linea con l'attuale concettualizzazione di documento informatico, come completata con la definizione di documento elettronico prevista dal Regolamento eIDAS. In tal senso, il documento informatico è il "contenuto" che si dovrebbe adattare a molti "contenitori" per essere formato, gestito e conservato, e che può avere, infatti, molti formati, molte firme, può essere oggetto di molti strumenti di trasmissione, ma ne devono essere comunque garantite la sicurezza, l'immodificabilità e l'integrità attraverso idonei sistemi di gestione e conservazione.

concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale". Anche tale articolo risulta ben coordinato con ciò che oggi possiamo considerare *ex lege* come documento (o dato) informatico[21].

Le definizioni sopra riportate di dato e documento in ambito digitale (contenute nella normativa europea e nazionale), infatti, comportano un superamento sostanziale del dualismo tra documento e dato, finendo per provocare ormai una coincidenza di fatto tra i due termini, qualora il dato contenga una rappresentazione affidabile di un fatto o atto giuridicamente rilevante.

Tale superamento concettuale si ritrova anche nelle recenti modifiche dell'eIDAS, laddove il nuovo art. 45 decies occupandosi degli effetti giuridici dei (nuovi) servizi fiduciari di archiviazione elettronica evidenzia che essi si riferiscono a dati e documenti. E la stessa definizione di archiviazione elettronica sembra far sfumare concettualmente il documento informatico in un dato affidabilmente archiviato, pur mantenendo formalmente una separazione tra dati e documenti nella sua parte testuale.

In eIDAS 2, infatti, l'archiviazione viene definita come un servizio che consenta la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità, nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione.

Tale impostazione terminologica ricorda da vicino ciò che in Italia da tempo viene considerato un sistema di conservazione "a norma" di documenti informatici, inteso come "insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti"[22]. In estrema sintesi, possiamo senz'altro sottolineare che l'Italia abbia fatto da apripista per favorire questa evoluzione del senso stesso e della necessità (oltre che dei modi e mezzi) di documentare affidabilmente nel mondo digitale e speriamo che riesca nei prossimi mesi a imporre le sue regole tecniche sui tavoli europei, nel momento in cui atti di esecuzione dovranno dettagliare la normativa più generale contenuta nel nuovo eIDAS[23].

---

[21] Nello specifico, dunque, il documento non deve essere necessariamente scritto o redatto sotto forma di un testo, bensì può essere ben costituito da un qualsiasi flusso di dati in forma elettronica: l'importante è che tale contenuto sia "stored", cioè reso statico e preservato nella sua integrità nel tempo.

[22] Glossario alle Linee Guida AgiD sulla formazione gestione e conservazione dei documenti informatici. Documenti normativi reperibili qui: https://www.agid.gov.it/it/linee-guida.

[23] Utile in tal senso la lettura del considerando 66 a eIDAS 2: "Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione elettronica sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e documenti elettronici, nonché per i servizi fiduciari associati. Al fine di garantire la certezza giuridica, la fiducia e l'armonizzazione in tutti gli Stati membri, è opportuno istituire un quadro giuridico per i servizi di archiviazione elettronica qualificati, ispirato al quadro per gli altri servizi fiduciari di cui al presente regolamento. Il quadro

L'approccio nazionale potrebbe portare la normativa europea a considerare così l'archiviazione come chiusura indispensabile del processo di formazione del documento informatico, come già è previsto leggendo gli articoli del CAD dedicati alla documentazione informatica (e alla conservazione) in combinato disposto con la regolamentazione tecnica contenuta nelle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Tale lettura sistematica può guidare l'attento interprete a considerare oggi i metadati obbligatori propri della fase di formazione come delle "proprietà" del documento, in grado di assicurare l'autenticità allo stesso, indispensabili quindi nella sua fase generativa. Questo corredo congenito è perciò utile a garantire una verifica successiva della sua paternità, attestandone con certezza l'origine. Si tratta di metadati che non esistono per essere già funzionali semplicemente alla sua ricercabilità, ma sono parte del DNA del documento e ne determinano le informazioni genetiche essenziali.

Insomma, finalmente si potrebbe avvertire anche in Europa una sana impostazione archivistica che possa garantire in ambiente digitale il vincolo (collegamento funzionale) tra i diversi documenti prodotti o ricevuti dall'ente pubblico e privato (e tra essi e il processo decisionale che li ha generati), superando quel monadismo documentale che ha gravemente pervaso in tutti questi anni la materia della digitalizzazione.

giuridico per i servizi di archiviazione elettronica qualificati dovrebbe offrire ai prestatori di servizi fiduciari e agli utenti un pacchetto di strumenti efficiente che comprenda requisiti funzionali per il servizio di archiviazione elettronica, nonché chiari effetti giuridici in caso di utilizzo di un servizio di archiviazione elettronica qualificato. Tali disposizioni dovrebbero applicarsi ai dati elettronici e ai documenti elettronici creati in forma elettronica e ai documenti cartacei che sono stati scannerizzati e digitalizzati. Ove necessario, tali disposizioni dovrebbero consentire che i dati elettronici e i documenti elettronici conservati siano trasferiti su supporti o formati diversi al fine di estenderne la durabilità e la leggibilità oltre il periodo di validità tecnologica, evitando nel contempo, nella misura del possibile, le perdite e le alterazioni. Quando i dati elettronici e i documenti elettronici trasmessi al servizio di archiviazione elettronica contengono una o più firme elettroniche qualificate ovvero uno o più sigilli elettronici qualificati, il servizio dovrebbe utilizzare procedure e tecnologie in grado di estendere la loro affidabilità per il periodo di conservazione di tali dati, eventualmente ricorrendo all'uso di altri servizi fiduciari qualificati istituiti dal presente regolamento. Per la creazione delle prove di conservazione in caso di utilizzo di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, è opportuno utilizzare servizi fiduciari qualificati. In relazione ai servizi di archiviazione elettronica non armonizzati dal presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni nazionali, in conformità del diritto dell'Unione, relative a tali servizi, quali disposizioni specifiche per i servizi integrati in un'organizzazione e utilizzati esclusivamente per gli archivi interni di tale organizzazione. Il presente regolamento non dovrebbe distinguere tra dati elettronici e i documenti elettronici creati in forma elettronica e documenti fisici che sono stati digitalizzati".

5. Conclusioni: il documento informatico a formazione progressiva in Italia e in Europa

In conclusione, è possibile riferire che il legislatore nazionale ha introdotto da tempo nella normativa primaria un modello di interazione giuridicamente rilevante che si basa su documenti informatici formati progressivamente all'interno di contesti riservati, previa idonea verifica dell'identità digitale degli utenti/cittadini/contraenti, prevedendo l'indispensabile associazione a tali documenti dei metadati necessari per qualificarne correttamente l'origine.

In questo modello nazionale rimane ovviamente essenziale garantire:

- una registrazione affidabile di tutto ciò che si manifesta on line;
- il presidio della volontà espressa attraverso un archivio informatico;
- la presenza di modelli di conservazione dei dati giuridicamente rilevanti, quali testimoni qualificati e fedeli dei fatti sviluppati on line.

Tale impostazione può trovare una autorevole e incredibile conferma dal legislatore di eIDAS 2.

In realtà, tale registrazione affidabile e archivisticamente corretta delle nostre azioni giuridicamente rilevanti che avvengono on line non costituisce nulla di nuovo. Si tratta infatti di una riedizione digitalmente significativa di quanto già la scienza diplomatica ammetteva nel periodo medievale per il confezionamento degli atti grazie alla presenza di un'autorità pubblica (previa identificazione degli attori, le cui sottoscrizioni rispondevano piuttosto all'adempimento di un mero formalismo). È il contesto archivistico, sviluppato attraverso rigorose regole tecniche e presidiato da qualificati responsabili, a garantire un sempre più evidente superamento delle formalità (di origine medievale[24]) in favore dell'evoluzione del documento informatico a "formazione progressiva".

E, in fin dei conti, sarà la qualità che dovrà governare il futuro delle nostre azioni informaticamente (e giuridicamente) rilevanti. È la qualità dei dati/documenti informatici che deve costituire, infatti, il presupposto necessario di qualsiasi futuro progetto di innovazione digitale, compresi i sistemi di intelligenza artificiale[25]. E la qualità si può ottenere soltanto attraverso un sofisticato contesto archivistico digitale.

Non si può non ricordare, in proposito, l'art. 6 del Decreto Legislativo 14 marzo 2013, n. 33 sul riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, il quale occupandosi di "qualità delle informazioni" precisa che le pubbliche amministrazioni garantiscono la qualità delle informazioni

[24] Si fa riferimento naturalmente alla genesi dell'atto notarile.

[25] Così Andrea Lisi e Sarah Ungaro, La protezione dei dati nei sistemi di intelligenza artificiale, in Atti della 8ª conferenza organizzativa degli archivi delle università italiane, Padova, Cleup, 2024.

riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti dalla legge, assicurandone l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, nonché la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità secondo quanto previsto dall'articolo 7.

Ognuna di queste esigenze può raggiungersi solo attraverso un buon sistema di gestione e conservazione di documenti informatici.

Occorre adesso spiegarlo con autorevolezza in Europa. I presupposti per poterlo fare ci sono tutti.

N. 4 - 2024 - pp. 54-61

European Digital Identity Wallet, nuova era del decennio digitale

Beatrice Tafini

Abstract [IT]: L'assenza di un quadro globale transfrontaliero o intersettoriale dell'UE in grado di garantire l'interoperabilità di un'identità digitale tra gli Stati membri ha spinto la Commissione europea a presentare una proposta di trasformazione digitale dell'Europa volta alla soppressione delle attuali frammentazioni derivanti da norme e standard divergenti. Tale proposta segna un passo importante e decisivo verso gli obiettivi del Decennio digitale 2030; in particolare, con l'introduzione del c.d. portafoglio digitale (anche solo "EDI Wallet"), la proposta della Commissione va nella direzione di voler garantire ai singoli cittadini il pieno controllo della propria identità nell'ecosistema digitale nel rispetto dei valori e dei diritti fondamentali dell'UE. Il presente articolo mira ad analizzare, seppur brevemente, la disciplina dei portafogli europei di identità digitale individuandone anche i risvolti che avranno sulla digitalizzazione dei servizi pubblici e privati. Risvolti che offrono un punto prospettico privilegiato per esaminare anche l'annosa questione sulla protezione dei dati personali degli utenti che assume un ruolo di cruciale importanza.

Abstract [EN]: The absence of a comprehensive cross-border or cross-sectoral EU framework capable of guaranteeing the interoperability of a digital identity between Member States has prompted the european Commission to present a proposal for the digital transformation of Europe aimed at eliminating the current fragmentation resulting from divergent rules and standards. This proposal marks an important and decisive step towards the goals of the Digital Decade 2030; in particular, with the introduction of the so-called digital wallet (also referred to as 'EDI Wallet'), the Commission's proposal goes in the direction of wanting to ensure that individual citizens are in full control of their identity in the digital ecosystem while respecting EU values and fundamental rights. This article aims to analyze, albeit briefly, the regulation of european digital identity wallets, also identifying the implications it will have on the digitization of public and private services. These implications offer a privileged perspective to examine also the long-standing issue of the protection of users' personal data, which is of crucial importance.

Parole Chiave: eIDAS, Portafoglio europeo, attributi, privacy, servizi digitali

Sommario: 1. Contesto normativo – 2. European Digital Identity Wallet – 3. Attestazioni elettroniche di attributi – 4. Protezione dati personali – 5. Considerazioni conclusive

1. Contesto normativo

Il 3 giugno 2021 la Commissione europea ha presentato una proposta (peraltro già approvata dal Parlamento europeo e quindi in attesa di approvazione anche da parte del Consiglio) di aggiornamento del quadro europeo dell'identità digitale, volta alla creazione di un quadro paneuropeo scevro dalle frammentazioni derivanti da una pletora di norme, sia a livello domestico sia a livello europeo che, in maniera più o meno parziale, tentano di regolamentarne la fattispecie.

La proposta di emendamento della Commissione europea al Regolamento del 23 luglio 2014 n. 910, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (*di seguito anche solo "Regolamento eIDAS"*)*, elaborato sulla scorta delle prescrizioni dettate dall'art. 49 del medesimo Regolamento*,* con l'introduzione del c.d. Portafoglio di identità digitale ("EUDI wallet"), contiene *in nuce* tutti gli elementi per consentire agli utenti di condividere in modo sicuro i dati relativi alla propria identità con fornitori di servizi online pubblici e privati utilizzando i propri dispositivi mobili, superando quindi l'eterogeneità dei sistemi giuridici nazionali.

Infatti, sebbene il predetto Regolamento abbia raggiunto molti degli obiettivi prefissati e sia diventato un elemento fondamentale per facilitare il mercato unico, la mancanza di un obbligo di notifica dei sistemi nazionali di identificazione elettronica e la limitatezza degli attributi, che possono essere comunicati in modo affidabile a terzi, recano in sé l'esigenza di definire un quadro normativo composito *in subiecta materia.*

Sul punto appare rilevante richiamare il Regolamento del 19 ottobre 2022 n.2065 c.d. Digital Acts, volto al corretto funzionamento del mercato interno dei servizi intermediari, il quale stabilisce norme armonizzate finalizzate alla realizzazione di un ambiente online sicuro, prevedibile e affidabile che possa facilitare l'innovazione pur assicurando ogni tutela ai diritti fondamentali.

In linea con il sopracitato Regolamento il Legislatore europeo, nel considerando 57 del novellato Regolamento eIDAS, stabilisce che laddove le piattaforme online di grandi dimensioni, come definite all'articolo 33 del Regolamento (UE) Digital Acts, richiedano agli utenti di autenticarsi per accedere ai servizi online dovranno, obbligatoriamente, accettare e agevolare anche l'uso del Portafoglio di identità digitale.

Si sottolinea che la volontà della Commissione di introdurre un'identità digitale affidabile, volontaria e controllata dall'utente, riconosciuta in tutta l'Unione pare, peraltro coerente con la recente *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, pubblicata dalla Commissione il 26 gennaio 2022 sotto l'egida della bussola digitale dell'UE.

In siffatto contesto del mercato unico digitale, viene quindi promossa una nuova realtà che pone al centro le persone e i loro diritti umani universali, attuando una maggiore autonomia e responsabilità nel pieno rispetto della sicurezza e della protezione dei diritti degli utenti.

Particolarmente significative in proposito appaiono le disposizioni, della summenzionata Dichiarazione europea, contenute nel capo II (che disciplina la solidarietà e inclusione) e nel capo V (che disciplina la sicurezza, protezione, autonomia e responsabilità), le quali, in coerenza con l'intero corpus normativo in materia e con le finalità sottese alla predetta dichiarazione, stabiliscono che l'identità digitale debba essere accessibile, affidabile, in grado di dare accesso ad un'ampia gamma di servizi online in totale sicurezza, inclusa la protezione dal furto e/o manipolazione dell'identità stessa.

Vi è poi un ulteriore elemento che conferma la vocazione della trasformazione digitale alla dimensione europea, orientata ai principi universali e unanimemente accettati. Ci si riferisce alla prescrizione imposta dalla normativa della Direttiva (UE) del 17 aprile 2019 n. 882 relativamente alla necessità di possedere *requisiti di accessibilità dei prodotti e dei servizi*. In tal senso il portafoglio europeo deve essere disponibile in un linguaggio semplice, comprensibile e accessibile alle persone con disabilità o con limitazioni funzionali.

2. European Digital Identity Wallet

A questo punto, nell'intento di proseguire il percorso di analisi sopra avviato, corre l'obbligo di esaminare la disciplina del portafoglio europeo di identità digitale.

Il Regolamento *de quo* definisce l'EUDI Wallet come "*un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati*".

In altri termini, i cittadini europei possono, gratuitamente, mediante tale strumento, condividere in modalità online e offline, con le c.d. *relying parties* o con il portafoglio europeo di un'altra persona, in maniera sicura e selettiva, i dati di identificazione personale (e se del caso ulteriori e/o diverse attestazioni elettroniche di attributi quali diplomi, licenze, certificati di nascita…) nonché sottoscrivere con firme elettroniche qualificate e/o apporre sigilli. La necessità dell'autenticazione in modalità offline è ravvisabile soprattutto in quei contesti per il quale sono previste interazioni *vis-à-vis*.

Senza volersi soffermare oltre sulle *relying parties,* pare *sufficiente* evidenziare che per quest'ultime si intendono tutte le persone fisiche e/o giuridiche che, previa registrazione presso lo stato membro in cui sono stabilite, fanno affidamento sui dati e/o gli attributi condivisi mediante i portafogli di identità digitale. Da sottolineare che tali soggetti, comunque, possono acquisire solo ed esclusivamente i dati per i quali sono stati autorizzati.

Le norme in esame prevedono che l'affidabilità e la conformità dell'EUDI Wal-

let vengano garantite dai singoli stati membri che, a tal fine, potranno: (i) emettere direttamente il portafoglio, (ii) incaricare un'organizzazione specifica ad emettere e gestire il portafoglio per suo conto, (iii) riconoscere il portafoglio emesso in modo indipendente da terzi.

In particolare, al fine di incoraggiare la digitalizzazione dei servizi del settore pubblico riducendo gli oneri amministrativi e sostenere la mobilità transfrontaliera per i cittadini e le imprese, si dovrebbe affermare l'applicazione del principio "*una tantum*", che consiste nel permettere ai cittadini e alle imprese di fornire gli stessi dati alle pubbliche amministrazioni una volta per tutte, senza necessità di doverne ripetere l'invio. L'applicazione di tale principio dovrebbe essere subordinata al consenso esplicito dell'utente e dovrebbe rispettare tutte le norme applicabili in materia di protezione dei dati, compresi i principi di minimizzazione dei dati, accuratezza, limitazione della conservazione, integrità e riservatezza, necessità, proporzionalità e limitazione delle finalità. A tal proposito è interessante segnalare la possibilità per l'utente di utilizzare il portafoglio europeo mediante uno pseudonimo a sua scelta. L'unico limite è costituito dai casi in cui il diniego all'utilizzo di uno pseudonimo sia previsto dal diritto unionale o dal diritto nazionale. Ne consegue che l'uso di servizi sotto pseudonimi deve essere sempre consentito e i fornitori di servizi non possono in alcun modo limitarlo mediante un contratto e/o condizioni d'uso del servizio stesso.

Orbene, l'intento di garantire un livello elevato di trasparenza e controllo da parte degli utenti sui loro dati, ha indotto inoltre il legislatore europeo a incentivare l'uso di un'interfaccia semplice ed intuitiva, la quale, come è noto, permette la condivisione di dati di identificazione o di attestazioni elettroniche di attributi in modo selettivo. A ciò si aggiunga l'obbligo per gli Stati membri di fornire mezzi idonei per revocare il portafoglio di identità digitale nei seguenti casi: (i) richiesta esplicita dell'utente; (ii) sicurezza compromessa in modo tale da pregiudicarne l'affidabilità; (iii) decesso dell'utente (o se persona giuridica cessazione dell'attività).

Dunque, nell'ottica di offrire una disciplina dell'identità digitale improntata all'armonizzazione massima tra le legislazioni nazionali, il regolatore non si è limitato a prescrivere disposizioni attinenti la struttura o la composizione del portafoglio, ma ha anche preso in considerazione e tenuto presente i livelli di garanzia originariamente riconosciuti alle identità digitali vigenti. Infatti, il connotato multilivello, caratteristico del contesto europeo in tale fattispecie, consiste proprio, oltre che nella totale assenza in alcuni Stati membri di soluzioni di identificazione elettronica, nella compresenza di una pluralità di regimi di identificazione elettronici notificati a norma dell'articolo 9, paragrafo 1, del regolamento (UE) n. 910/2014, caratterizzati da livelli di garanzia diversi (basso - significativo - elevato).

Sulla base di tale presupposto risulta evidente come il legislatore abbia dovuto trovare un bilanciamento tra l'esigenza di introdurre requisiti di sicurezza molto elevati e l'utilizzo nel nuovo portafoglio di strumenti di identificazione elettronica già esistenti e ampiamente utilizzati. Sul punto, le nuove previsioni normative sembrerebbero andare nella direzione di risolvere alcune lacune presenti nel precedente

testo legislativo. Infatti, secondo l'interpretazione letterale del testo in esame, gli utenti possono accedere al portafoglio europeo, utilizzando i propri mezzi di identificazione elettronica nazionale, anche se di livello "significativo" purché quest'ultimi siano combinati con ulteriori elementi di autenticazione che insieme siano in grado di soddisfare i requisiti del livello di garanzia "elevato".

In ultimo, per mera completezza di trattazione, si richiama, senza peraltro necessità di soffermarcisi, l"ampio dibattito, sviluppatosi intorno alla previsione normativa del regolamento in parola secondo la quale i portafogli europei di identità digitale devono offrire a tutte le persone fisiche la possibilità di firmare mediante firme elettroniche qualificate emesse a titolo gratuito, in particolare la questione che ha dato luogo a molteplici scritti e commenti attiene alla prevista gratuità.

3. Attestazioni elettroniche di attributi

Come si è avuto modo di evidenziare nel paragrafo precedente, la *ratio* dell'EUDI Wallet è quella di consentire a cittadini e imprese di condividere i dati e le informazioni personali in maniera sicura e agevole.

Proprio dal fondamento di tale corollario è scaturita l'esigenza di introdurre il servizio c.d. di attestazione elettronica di attributi che può essere erogato da: (i) prestatori di servizi fiduciari non qualificati (soggetti ai requisiti del regolamento eIDAS ma con attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni), (ii) prestatore di servizi fiduciari qualificati (prestatore di servizi fiduciari a cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato), (iii) (o per conto di) un ente del settore pubblico.

L'attributo viene definito dal Regolamento eIDAS come "*la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto",* in altri termini l'attributo concerne tutte quelle informazioni relative all'identità di una persona come qualifiche accademiche, compresi diplomi universitari o altri titoli di studio o qualifiche professionali.

Ebbene, in merito a quest'ultimo punto, il legislatore europeo, sempre nell'ottica di perseguire l'esigenza di certezza ha attribuito a tali attestazioni (purché provenienti da fornitori di servizi fiduciari qualificati o enti pubblici) i medesimi effetti giuridici che sono riconosciute alle attestazioni in formato cartaceo.

Tale assunto trova le sue ragioni nel fatto che ciascun Stato membro ha il dovere di individuare meccanismi adeguati, atti a permettere ai prestatori di servizi fiduciari qualificati di attingere direttamente alle c.d. "fonti autentiche" (archivi o sistemi, tenuti sotto la responsabilità di un ente del settore pubblico o privato, considerati una fonte primaria) per acquisire e/o convalidare gli attributi.

A questa specifica esigenza di certezza si deve la previsione normativa, la quale dispone che, qualora un attestato elettronico di attributi qualificato venga re-

vocato dopo l'iniziale rilascio, esso perda la propria validità solo ed esclusivamente dal momento della revoca e la sua situazione non può essere ripristinata in nessuna circostanza.

A tal proposito assume rilevanza anche il precetto relativo al mutuo riconoscimento tra gli Stati membri di un'attestazione elettronica qualificata di attributi. Infatti, un'attestazione elettronica qualificata di attributi fornita in uno Stato membro deve essere riconosciuta in tutti gli altri Stati membri.

Inoltre, indipendentemente dal fatto che il fornitore di attestazione sia un soggetto qualificato o non qualificato, le attestazioni di attributi hanno valore probante in procedimenti legali pur essendo costituite in formato elettronico.

Appare evidente, dal quadro così delineato, che il legislatore europeo ha ritenuto indispensabile ed indifferibile rafforzare le competenze digitali e sensibilizzare, in merito ai benefici e ai rischi dei portafogli europei di identità, i cittadini europei e nello specifico i gruppi vulnerabili (di cui fanno parte es. persone con disabilità, anziani), mediante programmi di formazione e campagne di comunicazione.

4. Protezione dati personali

Come sopra accennato, la proposta della commissione si inserisce in un ricco panorama normativo.

Con tale premessa, senza alcuna pretesa di esaustività, si tenterà, quindi di fermare l'attenzione sul rapporto tra EUDI Wallet e il Regolamento (UE) del 27 aprile 2016 n. 679 relativo *alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("GDPR").*

Sebbene lo scopo del GDPR sia quello di assicurare la libera circolazione dei dati personali tra gli Stati membri, è ampiamente riconosciuto che la diffusione delle informazioni debba avvenire nel rispetto dei diritti e libertà fondamentali delle persone fisiche. In quest'ottica si evidenzia che il sistema di tutela tracciato dalla proposta della Commissione è incentrato su due pilastri principali costituiti dal consenso dell'interessato e dal principio dell'*accountability*.

Partendo da queste considerazioni corre l'obbligo di segnalare che il consenso costituisce la prima e più significativa condizione di legittimità del trattamento per le operazioni eseguite mediante il portafoglio.

A tal proposito, il testo in esame dispone che gli utenti abbiano il pieno controllo del portafoglio e, di conseguenza, delle modalità di condivisione e utilizzo dei dati personali (definiti dall'art. 4 del summenzionato Regolamento).

La necessità di garantire il pieno controllo da parte degli utenti rende necessari diversi adempimenti procedurali sia da parte dei fornitori dell'EUDI Wallet sia da parte dei *Relying Parties*.

I fornitori dell'EUDI Wallet dovranno garantire la tutela dei dati personali fin dalla progettazione del trattamento mediante le note misure di "privacy by design"

e “privacy by default”. In altri termini, si rende necessario implementare idonee funzionalità di sicurezza avanzate per proteggere i dati personali da qualsiasi altra minaccia informatica come, ad esempio, furto d’identità o anche trattamenti non autorizzati o illeciti, perdita, distruzione e/o danno accidentale. Tali misure dovrebbero includere metodi di crittografia end-to-end e archiviazione all’avanguardia.

Un ulteriore prova a sostegno della forte attenzione mostrata nei confronti di tale disciplina relativa alla protezione dei dati, è riscontrabile nell’obbligo per i fornitori del portafoglio europeo di individuare delle misure atte ad agevolare l’utente nell’esercizio dei propri diritti come, ad esempio: il diritto alla cancellazione (“diritto all’oblio” ex art. 17 GDPR) dei propri dati personali, la possibilità di poter segnalare tempestivamente all’autorità nazionale competente in materia un presunto accesso e/o un uso illecito del portafoglio europeo e/o dei propri dati.

A garanzia di ulteriore maggior protezione, il legislatore ha previsto che lo Stato membro possa anche ritirare i portafogli europei nei casi di violazione o parziale compromissione dei portafogli stessi ove non vi si sia posto rimedio entro tre mesi dalla sospensione dell’utilizzo del portafoglio.

Inoltre, il testo in esame sembrerebbe garantire anche il principio di minimizzazione dei dati mediante la facoltà, per l’utente, di condividere con la parte che fa affidamento sull’ EUDI Wallet, solo ed esclusivamente i dati personali adeguati, pertinenti e limitati a quanto necessario per perseguire la specifica finalità per la quale sono richiesti.

Il pieno controllo dell’utente, si concretizza, inoltre, nel divieto, per il fornitore del portafoglio, di acquisire, combinare e, in ogni caso, trattare informazioni personali relative all’utente che non siano necessarie alla fornitura dei servizi del portafoglio stesso, salvo espressa richiesta dell’utente.

In particolare, è fatto espresso divieto, per il fornitore di attestazioni elettroniche di attributi, di combinare dati al fine di tracciare, collegare, correlare o comunque venire a conoscenza delle singole transazioni e/o del comportamento dell’utente.

Con riferimento alle modalità con cui tali dati devono essere mantenuti all’interno dell’EUDI Wallet, si ritiene sufficiente sottolineare, in aggiunta a quanto sopra, che i dati debbano essere tenuti logicamente separati tra di loro, che devono essere previsti metodi di cifratura e archiviazione all’avanguardia che siano accessibili solo all’utente e decifrabili solo da quest’ultimo, e che tali metodi si basino sulla comunicazione cifrata end-to-end con altri portafogli europei di identità digitale e parti facenti affidamento

In questo quadro, la Commissione stabilisce, inoltre, che le parti che fanno affidamento sul portafoglio europeo, devono rispettare le misure che più incarnano il principio dell’”*accountability*”, disposte dagli artt. 35 e 36 del GDPR, e cioè la valutazione d’impatto e l’eventuale consultazione preventiva all’Autorità di controllo.

Giova ricordare, infine, che la valutazione d’impatto deve essere compiuta prima di procedere al trattamento, e solo qualora l’esito dimostri l’esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento

deve procedere alla consultazione preventiva dell'Autorità di controllo.

Il legislatore nel delineare le tutele per gli utenti e i controinteressati ha opportunamente previsto la designazione da parte di ciascun stato membro di uno o più organismi di Vigilanza che hanno il compito di: (i) monitorare il rispetto della normativa vigente in materia mediante controlli ex ante ed ex post (sia in loco sia a distanza) nei confronti dei fornitori di portafogli, (ii) intervenire in caso di violazioni da parte dei fornitori dei portafogli, (iii) informare le autorità competenti responsabili della cybersicurezza in caso di violazioni e/o perdite di integrità, (iv) cooperare con le autorità di controllo di cui art. 51 GDPR, (vi) sospendere e/o imporre la cessazione della fornitura del portafoglio di identità laddove il fornitore non ottemperi alle indicazioni impartite.

5. Considerazioni conclusive

Approfondito il sostrato normativo di riferimento, si ritiene si possa affermare che alla Commissione europea vada riconosciuto il merito di aver definito un archetipo normativo volto ad eliminare l'evidente iato tra l'esigenza di certezza giuridica (e interoperabilità) nel contesto europeo e le previsioni normative dei singoli paesi membri.

Il Regolamento, così come verrà modificato dopo la definitiva approvazione della proposta, individua la cornice contenutistica minima che l'eventuale legislazione di settore è tenuta a disciplinare, limitando così la possibilità che si sviluppino normative nazionali speciali eccessivamente differenti fra loro.

L'auspicio è che il dialogo tra diritto interno e il diritto europeo offra nuovi spunti per l'analisi di un futuro digitale incentrato sulla persona.

N. 4 - 2024 - pp. 62-70

La protezione dei dati personali nell'architettura delPortafoglio Europeo

Sarah Ungaro

Abstract [IT]: Nella formulazione del Regolamento 2024/1183 (eIDAS 2) il Legislatore europeo ha potuto cogliere i benefici di un approfondito dibattito sul trattamento dei dati personali degli utenti da parte dei fornitori di tali servizi fiduciari o di eventuali terze parti coinvolte. In particolare, le soluzioni nell'ambito del quadro di interoperabilità di cui al testo del Regolamento eIDAS 2 sono conformi alle norme dell'Unione che stabiliscono i principi di protezione dei dati, quali la minimizzazione dei dati e il principio di limitazione delle finalità, e gli obblighi in materia, ad esempio la protezione dei dati fin dalla progettazione e per impostazione predefinita, specificandoli ulteriormente nel contesto di riferimento in cui viene inquadrato il trattamento dei dati personali.

Oltre a una diffusa declinazione dei diritti di controllo sui propri dati da parte degli utenti interessati al trattamento tramite i servizi fiduciari, al fine di assicurare concreta effettività al principio di limitazione delle finalità, le disposizioni di eIDAS 2 introducono le regole della dimostrazione "a conoscenza zero" e della "non osservabilità", che comporta che i fornitori di portafogli europei di identità digitale non possano vedere i dettagli delle transazioni effettuate dall'utente, fatto salvo il previo consenso esplicito dell'utente - per ciascuna specifica finalità e nel pieno rispetto delle norme del GDPR – e in linea, peraltro, con le osservazioni già formulate dall'EDPB (European Data Protection Board).

Abstract [EN]: In the formulation of the 2024/1183 Regulation (eIDAS 2), the European legislature was able to reap the benefits of an in-depth discussion on the processing of users' personal data by the trust service providers or any third parties involved. In particular, solutions under the interoperability framework set forth in the text of the eIDAS 2 Regulation comply with the Union's rules establishing data protection principles, such as data minimization and the purpose limitation principle, and data protection obligations, such as data protection by design and by default, by further specifying them in the framework in which the processing of personal data is framed.

In addition to widespread declination of the rights of users data subjects to control their own data through trust services, in order to ensure concrete effectiveness of the purpose limitation principle, the provisions of eIDAS 2 introduce the rules of "zero knowledge" proof and " unobservability" which implies that providers of European digital identity wallets cannot see the details of transactions made by

the user, except to the user's prior explicit consent - for each specific purpose and in full compliance with the regulations of the GDPR - and in line, moreover, with the comments already made by the European Data Protection Board (EDPB).

Parole chiave: eIDAS-2; GDPR; protezione dei dati personali; limitazione delle finalità; base giuridica.

Sommario: 1. Le nuove norme e i principi di protezione dei dati personali – 2. Limitazione delle finalità e divieto di combinazione dei dati trattati per altre finalità – 3. Punti di tangenza con i documenti di indirizzo dell'EDPB: le Linee guida 2/2019, le Linee guida 6/2020 e le Raccomandazioni 2/2021 – 4. Pannello di gestione per la condivisione dei dati e divulgazione selettiva – 5. Conclusioni

1. Le nuove norme e i principi di protezione dei dati personali

L'impostazione delle disposizioni contenute nella Proposta di Regolamento c.d. eIDAS 2[1] in materia di protezione dei dati personali rappresenta la sintesi di una più alta consapevolezza dei temi legati alla protezione dei dati, non solo perché – rispetto alla prima versione del Regolamento eIDAS (910/2014) [2] è entrato in vigore il Regolamento GDPR[3], ma soprattutto perché il Legislatore europeo ha potuto cogliere i benefici di un ampio e più maturo dibattito sui profili giuridici che si intersecano nell'utilizzo dei servizi fiduciari, a partire dai temi legati proprio alle finalità di utilizzo dei dati personali degli utenti da parte dei gestori di tali servizi o di eventuali terze parti coinvolte.

Tali riflessioni, ragionevolmente, hanno influenzato positivamente il Legislatore europeo nella stesura delle disposizioni della proposta di Regolamento eIDAS 2, in cui è possibile rintracciare non solo richiami formali al rispetto dei principi del GDPR, ma la sintesi di interlocuzioni maggiormente concrete, anche in relazione agli strumenti con cui assicurare agli utenti interessati una protezione dei dati effettiva, soprattutto considerando che tale proposta di Regolamento è in primis volta a disciplinare un mezzo di identificazione elettronica armonizzato, che consenta l'autenticazione e la condivisione dei dati collegati all'identità di persone fisiche e giuridiche[4].

---

[1] Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[2] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la Direttiva 1999/93/CE.

[3] Reg. UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR).

[4] Si veda, in proposito, il Considerando 7 della proposta di Regolamento eIDAS-2.

In effetti, già il citato Regolamento (UE) 2016/679 come anche la Direttiva 2002/58/CE[5] e il Regolamento (UE) 2018/1725[6] si applicano a tutte le attività di trattamento dei dati personali ai sensi del Regolamento (UE) n. 910/2014, pertanto, anche le soluzioni nell'ambito del quadro di interoperabilità di cui alla proposta di Regolamento eIDAS 2 sono conformi alle norme dell'Unione che stabiliscono principi di protezione dei dati, quali la minimizzazione dei dati e il principio di limitazione delle finalità, e obblighi in materia, ad esempio la protezione dei dati fin dalla progettazione e per impostazione predefinita[7], specificandoli ulteriormente nel contesto di riferimento in cui viene inquadrato il trattamento dei dati personali.

2. Limitazione delle finalità e divieto di combinazione dei dati trattati per altre finalità

In tale prospettiva, con specifico riferimento al principio di limitazione delle finalità, sancito all'art. 5, par. 1, lett. b), del GDPR, il Considerando 12 della proposta di Regolamento eIDAS 2 declina in modo diretto e specifico tale principio, chiarendo che dovrebbero essere stabilite garanzie puntuali al fine di impedire ai fornitori di mezzi di identificazione elettronica e di attestati elettronici di attributi di combinare i dati personali ottenuti nella prestazione di altri servizi con i dati personali trattati al fine della prestazione dei servizi che rientrano nell'ambito di applicazione del Regolamento. In particolare, i dati personali relativi alla fornitura dei portafogli europei di identità digitale dovrebbero essere tenuti logicamente separati dagli altri dati detenuti dal fornitore del portafoglio europeo di identità digitale.

Nello specifico, inoltre, si evidenzia che l'utilizzo gratuito dei portafogli europei di identità digitale non comporta la possibilità per un fornitore di servizi di poter trattare dati ulteriori rispetto a quanto necessario per la fornitura dei servizi dei portafogli europei di identità digitale, poiché le norme della proposta di Regolamento eIDAS 2 non consentono il trattamento, da parte del fornitore del portafoglio europeo di identità digitale, dei dati personali conservati nel portafoglio europeo di identità digitale o risultanti dall'uso dello stesso, se non ai fini della fornitura dei servizi dei portafogli europei di identità digitale.

Al fine di assicurare concreta effettività al principio di limitazione delle finalità,

---

[5] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), c.d. Direttiva e-privacy.

[6] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[7] Per approfondimenti, cfr. il Considerando 9 della proposta di Regolamento eIDAS-2.

lo stesso testo introduce la regola della "non osservabilità", sulla scorta del quale, per garantire la tutela della vita privata, i fornitori di portafogli europei di identità digitale dovrebbero garantire di evitare di raccogliere dati e di avere accesso e conoscenza delle transazioni degli utenti del portafoglio europeo di identità digitale. Tale regola della "non osservabilità" comporta che i fornitori non possano vedere i dettagli delle transazioni effettuate dall'utente. In casi specifici, tuttavia, sulla base del previo consenso esplicito dell'utente - per ciascuna specifica finalità e nel pieno rispetto delle norme del GDPR - ai fornitori di portafogli europei di identità digitale potrebbe essere concesso l'accesso alle informazioni necessarie per la fornitura di un particolare servizio connesso ai portafogli europei di identità digitale[8].

3. Punti di tangenza con i documenti di indirizzo dell'EDPB: le Linee guida 2/2019, le Linee guida 6/2020 e le Raccomandazioni 2/2021

In relazione a tali elementi, il Legislatore della proposta di Regolamento eIDAS 2 sembra aver accolto le riflessioni formulate dall'European Data Protection Board (EDPB) espresse in alcuni documenti di indirizzo.

Ci si riferisce, in particolare, alle Linee guida 2/2019[9], alle Linee guida 6/2020[10] e alle Raccomandazioni 2/2021[11].

In tali documenti l'EDPB chiarisce la necessità di tenere correttamente distinti il trattamento dei dati che siano strettamente necessari all'erogazione del servizio richiesto e che, in quanto tale, è sorretto dalla base giuridica di cui all'art. 6, par. 1, lett. b) del GDPR (ossia, nei casi in cui il trattamento risulti necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrat-

[8] Si veda il Considerando 32 della proposta di Regolamento eIDAS-2 e l'art. 5 bis, par. 14, della proposta di Regolamento eIDAS-2. In ogni caso, risulta utile evidenziare che, mentre il Considerando 32 riporta il requisito del consenso espresso, la formulazione dell'art. 5-bis, par. 14, richiede addirittura che sia l'utente a richiedere espressamente che il fornitore del portafoglio europeo di identità digitale possa raccogliere informazioni relative all'uso dello stesso portafoglio europeo che non sono necessarie per la prestazione dei servizi di identità digitale, o combinare i dati di identificazione personale dell'utente con altri dati personali conservati nel portafoglio europeo o relativi al suo uso con i dati personali provenienti da altri servizi offerti dallo stesso fornitore o da terzi che non sono necessari per la prestazione dei servizi del portafoglio europeo di identità digitale.

[9] Linee guida EDPB 272019 sul trattamento dei dati personali ai sensi dell'art. 6, paragrafo 1, lettera b) del Regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati. Versione 2.0 (adottate in data 8 ottobre 2019).

[10] Linee guida EDPB 6/2020 sull'interazione tra la seconda Direttiva sui servizi di pagamento e il GDPR. Versione 2.0 (adottate il 15 dicembre 2020).

[11] Raccomandazioni 2/2021 EDPB sulla base giuridica per la conservazione dei dati delle carte di credito al solo scopo di agevolare ulteriori operazioni online (adottate il 19 maggio 2021).

tuali adottate su richiesta dello stesso), dai trattamenti che risultino ulteriori e che, pertanto, dovranno essere sorretti da un'ulteriore base giuridica, ai sensi dell'art. 6 GDPR, per essere considerati leciti.

Sul punto, nelle Linee guida 2/2019, l'EDPB chiarisce che "se il trattamento non è considerato «necessario all'esecuzione di un contratto», ossia quando un servizio richiesto può essere prestato senza lo svolgimento del trattamento specifico, il Comitato europeo per la protezione dei dati riconosce che può essere applicabile un'altra base giuridica, purché siano soddisfatte le condizioni pertinenti. In particolare, in determinate circostanze, può essere più opportuno basarsi sul consenso liberamente espresso ai sensi dell'articolo 6, paragrafo 1, lettera a). In altri casi, l'articolo 6, paragrafo 1, lettera f), può costituire un fondamento di liceità più idoneo per il trattamento. La base giuridica deve essere individuata prima dell'attuazione del trattamento e deve essere specificata nelle informazioni fornite agli interessati conformemente agli articoli 13 e 14 (*n.d.r.* del GDPR)"[12].

In effetti, secondo l'EDPB, nel rispetto degli obblighi in materia di trasparenza, i titolari del trattamento dovrebbero assicurarsi di evitare qualsiasi confusione riguardo alla base giuridica applicabile, soprattutto quando quella appropriata è individuata nell'articolo 6, paragrafo 1, lettera b), e gli interessati stipulano un contratto relativo a servizi online. A seconda delle circostanze, infatti, gli interessati possono erroneamente avere l'impressione di esprimere un consenso in linea con l'articolo 6, paragrafo 1, lettera a), firmando un contratto o accettando condizioni di servizio. Al tempo stesso, un titolare del trattamento potrebbe erroneamente presumere che la firma di un contratto corrisponda a una manifestazione di consenso ai sensi dell'articolo 6, paragrafo 1, lettera a).

Tuttavia, l'EDPB sottolinea che si tratta di concetti assolutamente diversi ed è importante distinguere tra l'accettazione di condizioni di servizio ai fini della conclusione di un contratto e la prestazione di un consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), dato che tali concetti hanno requisiti e conseguenze giuridiche diversi[13].

Tali indicazioni risultano particolarmente rilevanti in tema di disposizioni in materia di servizi fiduciari, nell'ottica dei servizi disciplinati dalla Proposta di regolamento eIDAS 2, in riferimento ai trattamenti di dati personali posti in essere dai prestatori di servizi fiduciari relativamente alla finalità di sicurezza e di prevenzione delle frodi. Sul punto, infatti, le Linee guida EDPB 2/2019 precisano che "il trattamento per finalità di prevenzione delle frodi può comportare il monitoraggio e la profilazione dei clienti. Secondo il Comitato europeo per la protezione dei dati è probabile che tale trattamento ecceda quanto oggettivamente necessario all'esecuzione di un contratto stipulato con un interessato. Tuttavia il trattamento dei dati personali strettamente necessario per finalità di prevenzione delle frodi può costituire un le-

[12] Si veda par. 17 delle Linee guida EDPB 2/2019.

[13] Cfr. par. 20 delle stesse Linee guida.

gittimo interesse del titolare del trattamento (*n.d.r.* il prestatore di servizi fiduciari in riferimento a eIDAS 2) e può quindi essere considerato lecito se il titolare soddisfa i requisiti specifici di cui all'articolo 6, paragrafo 1, lettera f) (legittimo interesse). Inoltre, anche l'articolo 6, paragrafo 1, lettera c) (osservanza di un obbligo legale) potrebbe costituire una base giuridica per il trattamento in questione".

Tuttavia, con specifico riferimento ai servizi fiduciari, compresi quelli disciplinati nella proposta di regolamento eIDAS 2, a parere di chi scrive, risulterebbe maggiormente corretto individuare per i trattamenti di dati personali aventi la finalità di prevenzione delle frodi nell'ambito degli stessi servizi fiduciari la base giuridica di cui alla lett. e) del par. 1, art. 6, del GDPR, ossia l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

Inoltre, in merito alla già citata regola della "non osservabilità", in base alla quale i fornitori di portafogli europei di identità digitale dovrebbero evitare di raccogliere dati e di avere accesso e conoscenza delle transazioni degli utenti del portafoglio europeo di identità digitale, è opportuno menzionare quanto specificato nelle Linee guida 6/2020 dell'EDPB, sull'interazione tra la seconda Direttiva sui servizi di pagamento e il GDPR. Nello specifico, al cap. 5, l'EDPB ricorda che anche singole transazioni o operazioni online possono rivelare informazioni sensibili su un singolo interessato, comprese quelle relative a categorie particolari di dati personali.

Pertanto, qualora i trattamenti di dati personali effettuati dai prestatori nell'ambito dei servizi fiduciari di eIDAS 2 si dovessero intersecare con altri che risultino finalizzati ad attività di profilazione - ad es. quelli obbligatoriamente previsti nell'ambito della Direttiva PSD-2[14] – ciò potrebbe determinare anche il trattamento di dati appartenenti a categorie particolari, desumendoli da dati che di per sé non appartengono a categorie particolari, ma che diventano tali se combinati con altri dati.

Da ultimo, su tali profili, appare utile considerare quanto specificato dallo stesso EDPB nelle Raccomandazioni 2/2021, con specifico riferimento alla base giuridica per la conservazione dei dati delle carte di credito al solo scopo di agevolare ulteriori operazioni online. In particolare, l'EDPB chiarisce che "il titolare del trattamento (*n.d.r.* prestatore di servizi) deve disporre di una base giuridica valida ai sensi dell'articolo 6 del RGPD per conservare tali dati. Al riguardo, va osservato che alcune delle basi giuridiche di cui all'articolo 6 del RGPD non sarebbero applicabili alla situazione in esame e devono essere escluse. La conservazione dei dati della carta di credito successivamente a una transazione, al fine di facilitare ulteriori acquisti, non può essere considerata necessaria per l'adempimento di un obbligo legale (articolo 6, paragrafo 1, lettera c), RGPD), né per la salvaguardia degli interessi vitali di una persona fisica (articolo 6, paragrafo 1, lettera d), RGPD). Nemmeno l'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è in-

[14] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 dicembre 2015 che abroga la Direttiva 2007/64/CE e stabilisce nuove norme per garantire certezza giuridica ai consumatori, ai commercianti e alle imprese nella catena di pagamento e per modernizzare il quadro giuridico riguardante il mercato dei servizi di pagamento.

vestito il titolare del trattamento (articolo 6, paragrafo 1, lettera e), RGPD) può essere considerata una base giuridica idonea (*omissis*). Le considerazioni che precedono portano a concludere che il consenso (articolo 6, paragrafo 1, lettera a), RGPD) sembra essere l'unica base giuridica idonea ad assicurare la liceità del trattamento sopra descritto. Infatti, al fine di gestire i rischi per la sicurezza, consentire all'interessato di mantenere il controllo sui propri dati e decidere attivamente in merito all'uso dei dati relativi al credito, è opportuno ottenere il consenso specifico dell'interessato prima di conservare i dati della sua carta di credito dopo un acquisto".

Per quanto riguarda i trattamento di dati personali diversi dalla conservazione, e tuttavia in linea con tale approccio, si rileva che il già citato Considerando 32 della proposta di regolamento eIDAS 2 specifica che la menzionata regola di "non osservabilità" comporta che i fornitori non possano vedere i dettagli delle transazioni effettuate dall'utente, fatto salvo il previo consenso esplicito dell'utente - per ciascuna specifica finalità e nel pieno rispetto delle norme del GDPR - ai fornitori di portafogli europei di identità digitale.

4. Pannello di gestione per la condivisione dei dati e divulgazione selettiva

I diritti di controllo sui propri dati personali da parte degli interessati nelle disposizioni della proposta di Regolamento eIDAS 2 sono enfatizzati in diverse disposizioni, che declinano specificamente il diritto di poter richiedere, selezionare, combinare, conservare, cancellare, condividere e presentare in sicurezza i dati relativi alla loro identità e richiedere la cancellazione dei loro dati personali in modo pratico e intuitivo, con il controllo esclusivo dell'utente, consentendo al contempo la divulgazione selettiva dei dati personali, in particolare utilizzando un pannello di gestione comune dei dati.

Nello specifico, nella proposta si introduce un'importante novità in tal senso, poiché i portafogli europei di identità digitale dovrebbero disporre, tra le proprie funzioni, di un pannello di gestione comune incorporato nella progettazione, al fine di garantire un livello più elevato di trasparenza, di tutela della vita privata e di controllo sui dati personali da parte degli utenti. Tale funzione dovrebbe prevedere un'interfaccia semplice e di facile utilizzo con una panoramica di tutte le parti facenti affidamento sulla certificazione con cui l'utente condivide dati, inclusi gli attributi, e del tipo di dati condivisi con ciascuna parte facente affidamento sulla certificazione. Tale pannello di gestione, da attivarsi per impostazione predefinita, dovrebbe consentire agli utenti di tracciare tutte le transazioni eseguite tramite il portafoglio europeo di identità digitale con almeno i seguenti dati: l'ora e la data della transazione, l'identificazione della controparte, i dati personali richiesti e i dati condivisi. Queste informazioni dovrebbero essere memorizzate anche se la transazione non è

stata conclusa e ne deve essere assicurata l'integrità e l'inalterabilità, in modo che non sia possibile contestare l'autenticità delle informazioni contenute nella cronologia delle transazioni. In particolare, il pannello di gestione dovrebbe consentire agli utenti di chiedere facilmente che una parte facente affidamento sulla certificazione cancelli immediatamente dati personali ai sensi dell'articolo 17 del GDPR e di segnalare facilmente la parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente, in caso di ricezione di una richiesta di dati personali asseritamente illecita o sospetta, direttamente tramite il portafoglio europeo di identità digitale[15].

Tali accentuati poteri di controllo in relazione ai dati a cui è possibile avere accesso risultano anche dalle disposizioni in base alle quali, ai fini della registrazione, le parti facenti affidamento sulla certificazione dovrebbero fornire le informazioni necessarie a consentire la loro identificazione e autenticazione elettroniche nei portafogli europei di identità digitale. Nel dichiarare l'uso previsto del portafoglio europeo di identità digitale, le parti facenti affidamento sulla certificazione dovrebbero fornire informazioni in merito ai dati che richiederanno, se del caso, ai fini della prestazione dei loro servizi come anche il motivo della richiesta. Fatti salvi, ovviamente gli obblighi di informativa ai sensi degli artt. 13-14 del GDPR e di valutazione d'impatto sulla protezione dei dati, di cui all'art. 35 GDPR.

Nell'ambito dei poteri di controllo dell'utente interessato al trattamento, occorre annoverare anche la possibilità di divulgazione selettiva, che conferisce al soggetto a cui i dati si riferiscono il potere di divulgare solo alcune parti di un insieme di dati più ampio, affinché il soggetto ricevente ottenga solo le informazioni necessarie per la prestazione di un servizio richiesto da un utente. Nello specifico, il portafoglio europeo di identità digitale dovrebbe consentire, a livello tecnico, la divulgazione selettiva degli attributi alle parti facenti affidamento sulla certificazione, in modo che per l'utente sia tecnicamente possibile divulgare selettivamente gli attributi, anche quando in origine sono parti di una serie di attestati elettronici distinti, e combinarli e presentarli senza soluzione di continuità alle parti facenti affidamento sulla certificazione. Tale caratteristica dovrebbe diventare una caratteristica di progettazione di base dei portafogli europei di identità digitale, rafforzando in tal modo la praticità e la tutela dei dati personali, compresa la minimizzazione dei dati[16].

In tale ottica si inserisce anche il principio della dimostrazione "a conoscenza zero", che implica la necessaria integrazione nel portafoglio europeo di identità digitale di diverse tecnologie che preservino la riservatezza, utilizzando metodi crittografici in grado di consentire a una parte facente affidamento sulla certificazione di convalidare la veridicità di una determinata dichiarazione sulla base dei dati di identificazione e dell'attestato di attributi della persona in questione, senza rivelare alcun dato su cui si basa tale dichiarazione, così da preservare la riservatezza dei

[15] Si veda il Considerando 13 e l'art. 5 bis della proposta di Regolamento eIDAS-2.

[16] Per approfondimenti, Considerando 59.

dati dell'utente[17].

5. Conclusioni

Nella proposta di Regolamento eIDAS 2 il Legislatore europeo ha introdotto regole e strumenti che rappresentano un maturo livello di evoluzione nella protezione dei dati personali: in particolare, la disciplina del portafoglio europeo di identità digitale è tesa a garantire il massimo livello di protezione e sicurezza dei dati ai fini dell'identificazione e autenticazione elettroniche, per agevolare l'accesso a servizi pubblici e privati (indipendentemente dal fatto che tali dati siano conservati localmente o attraverso soluzioni basate sul cloud), tenendo debitamente conto dei diversi livelli di rischio e garantendo concretamente il rispetto dei principi di minimizzazione dei dati e di limitazione delle finalità, nonché di protezione dei dati fin dalla progettazione e per impostazione predefinita, specificandoli ulteriormente in relazione alle misure di sicurezza[18] per il trattamento dei dati personali nel contesto di riferimento.

[17] Cfr. Considerando 13.

[18] Nella proposta di regolamento in commento, si ritrovano diffusi richiami non solo all'applicazione di misure di cibersicurezza e alla crittografia, ma anche all'adozione di misure supplementari che contribuiscano alla protezione dei dati personali, quali ad es. la separazione fisica dei dati personali relativi alla fornitura dei portafogli europei di identità digitale da qualsiasi altro dato detenuto dal fornitore.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 71-80

Il ruolo degli standard in eIDAS2

Andrea Caccia

Abstract: si analizza l'evoluzione del ruolo degli standard nel contesto della revisione del Regolamento eIDAS (electronic IDentification, Authentication and trust Services), introdotta col Regolamento (UE) 2024/1183 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale e denominata comunemente eIDAS2. L'attenzione dell'articolo si concentra in particolare sull'utilizzo degli standard nell'ambito dell'European Digital Identity Wallet (EUDI Wallet) e dei servizi fiduciari, esaminando le differenze rispetto all'approccio adottato nella versione precedente del Regolamento. Vengono inoltre analizzate le implicazioni di tali cambiamenti per i diversi stakeholder, includendo fornitori di servizi, pubbliche amministrazioni e utenti finali, sia imprese che cittadini.

Introduzione

Il Regolamento eIDAS (electronic IDentification, Authentication and trust Services) ha rappresentato un punto di svolta per il mercato unico digitale europeo, gettando le basi per l'interoperabilità e la fiducia nei servizi di identificazione elettronica e nei servizi fiduciari. Al fine di migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere identità digitali affidabili per tutti i cittadini europei nel rispetto degli obiettivi del programma strategico per il decennio digitale 2030, istituito dalla decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, si è resa necessaria una revisione del Regolamento eIDAS. È stato dunque pubblicato il 30 aprile 2024 il Regolamento (UE) 2024/1183, che qui di seguito sarà indicato come "eIDAS2", che modifica il Regolamento (UE) n. 910/2014 (eIDAS) introducendo il Portafoglio d'Identità Europeo (European Digital Identity Wallet o EUDI Wallet) ed estendento significativamente anche i servizi fiduciari.

Gli standard europei giocano un ruolo fondamentale per l'attuazione di eIDAS2, ancora più importante di quanto già avveniva con la versione precedente del Regolamento, che dovranno evolvere tenendo conto delle novità normative per assicurare che i Wallet di identità digitale e i servizi fiduciari non solo soddisfino le

esigenze tecnologiche attuali ma siano anche sufficientemente robusti per proteggere l'identità digitale e le transazioni di milioni di europei.

L'evoluzione del ruolo degli standard in eIDAS2

Si è scelto di utilizzare nell'articolo il termine "standard" invece di "norma", sebbene quest'ultimo sia il termine che si trova nel Regolamento e utilizzato nei contesti formali per riferirsi a specifiche tecniche o procedurali adottate da un'organizzazione di standardizzazione riconosciuta. Sebbene si sia optato per l'uso del termine d'uso più comune "standard" per rendere il contenuto più facilmente accessibile, tale termine è da intendersi come sinonimo di «norma» in questo articolo.

Nella versione originale del Regolamento eIDAS in vigore fino al 20 maggio 2024, gli standard svolgevano già un ruolo importante nel garantire l'interoperabilità e la sicurezza dei servizi di identificazione elettronica e dei servizi fiduciari. Tuttavia, eIDAS2 introduce un approccio più sistematico e armonizzato all'uso degli standard, con l'obiettivo di rafforzare ulteriormente la fiducia e l'uniformità nell'applicazione dei requisiti del Regolamento a livello europeo.

Una delle principali novità di eIDAS2 è l'obbligatorietà di emissione da parte della Commissione di atti d'esecuzione sia per il portafoglio di identità che per i servizi fiduciari. Per tali atti c'è in quasi tutti i casi l'obbligo di stabilire un elenco di standard di riferimento affiancato, ove necessario, da specifiche e procedure definiti dalla Commissione. Questo approccio offre una maggiore flessibilità rispetto alla sola indicazione di standard, consentendo di adattarsi più rapidamente all'evoluzione tecnologica e alle esigenze del mercato.

Inoltre, eIDAS2 prevede una presunzione di conformità ai requisiti del Regolamento laddove siano rispettati gli standard, le specifiche e le procedure indicati negli atti di esecuzione. Ciò rafforza il ruolo degli standard individuati e ne promuove l'adozione da parte degli operatori del settore.

L'EUDI Wallet rappresenta una delle principali innovazioni introdotte da eIDAS2. Si tratta di uno strumento digitale che consentirà ai cittadini e alle imprese di conservare e gestire in modo sicuro le proprie identità digitali, le credenziali e gli attributi, e di utilizzarli per accedere a servizi online pubblici e privati in tutta l'UE.

Gli standard svolgeranno un ruolo cruciale nel garantire l'interoperabilità, la sicurezza e la privacy degli EUDI Wallet. eIDAS2 prevede l'adozione di atti di esecuzione entro 6 mesi dall'entrata in vigore del Regolamento per stabilire requisiti, standard, specifiche e procedure per l'implementazione degli EUDI Wallet, nonché per la loro certificazione e la pubblicazione di informazioni sui wallet certificati.

Questo approccio armonizzato agli standard favorirà lo sviluppo di EUDI Wallet interoperabili e affidabili, facilitando la loro adozione su larga scala e contribuendo alla creazione di un ecosistema digitale europeo più integrato e sicuro.

Quanto ai servizi fiduciari, sia qualificati che non qualificati, eIDAS2 rafforza

anche il ruolo degli standard anche in questo contesto. Per i servizi fiduciari non qualificati, il Regolamento introduce nuovi requisiti in materia di sicurezza e notifica delle violazioni cpn uno specifico articolo, il 19 bis, prevedendo anche in questo caso l'adozione di atti di esecuzione entro 12 mesi per stabilire standard, specifiche e procedure di riferimento.

Per quanto riguarda i servizi fiduciari qualificati, eIDAS2 prevede l'adozione di atti di esecuzione entro 12 mesi per definire standard, specifiche e procedure in diverse aree, tra cui la verifica dell'identità e degli attributi, la gestione dei dispositivi di creazione di firme e sigilli elettronici qualificati a distanza, la convalida e la conservazione delle firme elettroniche qualificate, e i servizi di recapito elettronico certificato e di archiviazione elettronica.

Questo approccio armonizzato agli standard contribuisce a garantire un elevato livello di sicurezza, affidabilità e interoperabilità dei servizi fiduciari in tutta l'UE, rafforzando la fiducia degli utenti e favorendo l'adozione di soluzioni digitali avanzate.

L'evoluzione del ruolo degli standard in eIDAS2 avrà importanti implicazioni per i diversi stakeholder:

- I fornitori di servizi dovranno adeguarsi ai nuovi requisiti e standard previsti dal Regolamento, investendo nell'aggiornamento delle proprie soluzioni tecnologiche e dei processi operativi. Tuttavia, l'armonizzazione degli standard a livello europeo offrirà anche nuove opportunità di business, facilitando l'accesso a un mercato più ampio e integrato, fine ultimo della regolamentazione europea.
- Le pubbliche amministrazioni dovranno adattare i propri sistemi e servizi per garantire la compatibilità con gli EUDI Wallet e con i nuovi standard previsti per i servizi fiduciari. In particolare, in Italia, è prevista la sostituzione della PEC con un servizio elettronico di recapito certificato qualificato basato su standard, in conformità alle nuove Regole tecniche dell'AGID. Ciò richiederà investimenti, ma, anche grazie alla maggiore concorrenza, consentirà di offrire servizi più efficienti, sicuri e user-friendly ai cittadini e alle imprese.
- Per gli utenti finali, sia cittadini che imprese, l'adozione di standard si tradurrà in una maggiore facilità d'uso, sicurezza e privacy nell'accesso ai servizi digitali. I portafogli europei di identità digitale, in particolare, offriranno un modo semplice e affidabile per gestire le identità digitali e interagire con le pubbliche amministrazioni e le imprese online. In particolare si segnala l'introduzione in Italia del sistema "IT Wallet" col decreto-legge 2 marzo 2024, n. 19, che ha una fase di attuazione molto sfidante che anticiperà di qualche mese l'iniziativa europea per poi convergere sull'applicazione delle regole europee nei tempi previsti da eIDAS2.

Esaminiamo ora in dettaglio i passaggi più importanti dell'attuazione di eIDAS2 che sono legati all'adozione degli atti d'esecuzione.

Gli atti di esecuzione da emanare entro il 21 novembre 2024 (6 mesi dall'entrata in vigore)

eIDAS2 prevede l'adozione di numerosi atti di esecuzione da parte della Commissione europea entro il 21 novembre 2024, a 6 mesi dall'entrata in vigore del Regolamento, con l'obiettivo di definire standard, specifiche e procedure in diverse aree chiave, in particolare per quanto riguarda l'implementazione e la certificazione dei portafogli europei di identità digitale (in inglese European Digital Identity Wallet, abbreviato in "EUDI Wallet") e le attestazioni elettroniche di attributo.

Tra gli atti di esecuzione più rilevanti da adottare entro questo termine, troviamo quelli relativi ai requisiti, agli standard e alle procedure per l'implementazione degli EUDI Wallet (Articolo 5 bis, paragrafo 23), alle specifiche e procedure per fornitori di servizi che intendo utilizzare gli EUDI Wallet, indicati nella versione italiana di eIDAS2 come "parti facenti affidamento sulla certificazione dei portafogli europei di identità digitale", (Articolo 5 ter, paragrafo 11), e agli standard e alle procedure per la certificazione degli EUDI Wallet (Articolo 5 quater, paragrafo 6). Questi atti di esecuzione saranno fondamentali per garantire l'interoperabilità, la sicurezza e la privacy degli EUDI Wallet, favorendone l'adozione su larga scala.

Si noti che nel caso degli atti riguardanti i fornitori di servizio che intendono utilizzare gli EUDI Wallet manca l'obbligo di pubblicazione di un elenco di standard anche se, secondo la personale opinione di chi scrive, sarebbe invece importante l'adozione di standard che potrebbero essere più adatti alle esigenze del mercato grazie al più facile coinvolgimento degli stakeholder, soprattutto nel caso di piccole e medie imprese, negli enti di standardizzazione.

Altri atti di esecuzione da adottare entro 6 mesi riguardano le attestazioni elettroniche di attributi, con particolare attenzione agli standard e alle procedure per le attestazioni elettroniche di attributo qualificate (Articolo 45 quinquies, paragrafo 5), per il catalogo degli attributi e per gli schemi di attestazione e verifica (Articolo 45 sexies, paragrafo 2), e per le attestazioni rilasciate da organismi del settore pubblico (Articolo 45 septies, paragrafi 6 e 7).

Le attestazioni di attributo sono attestazioni associate a persone fisiche o giuridiche: ad esempio, rispettivamente, una patente di guida per una persona fisica oppure l'iscrizione alla camera di commercio per una persona giuridica. Le attestazioni rappresentano il contenuto principale previsto per i portafogli di identità digitale, sia quello europeo che quello italiano. eIDAS2 prevede due modalità di emissione di tali attestazioni: da parte di un particolare tipo di prestatore di servizi fiduciari, in modo del tutto simile all'emissione di certificati associati alla firma digitale, oppure da parte (o per conto) di un organismo del settore pubblico responsabile di una fonte autentica, negli esempi fatti il Ministero dei trasporti è la fonte autentica per le patenti di guida mentre le Camere di commercio lo sono per la relativa iscrizione. Le attestazioni emesse come servizio fiduciario sono soggette alle regole generali di tali servizi e, in particolare, la vigilanza, nel caso invece di attestazioni emesse da un

soggetto pubblico, o per suo conto, è prevista la notifica alla Commissione europea. In entrambi i casi è comunque necessario ottenere un rapporto di conformità di terza parte da parte di un organismo accreditato.

L'adozione tempestiva di questi atti di esecuzione sarà cruciale per l'effettiva attuazione delle novità introdotte da eIDAS2, in quanto fornirà agli operatori del settore e alle pubbliche amministrazioni un quadro di riferimento chiaro e armonizzato per lo sviluppo e l'implementazione di soluzioni interoperabili e conformi ai requisiti del Regolamento.

Sarà importante partecipare al processo di elaborazione degli standard che dovranno essere di supporto agli atti di esecuzione, al fine di garantire che siano effettivamente in grado di rispondere a tutti i requisiti trovando il giusto equilibrio: da un lato rispondere alle esigenze stringenti di conformità alla normativa sul trattamento dei dati personali e, dall'altro, alle esigenze di business del mercato garantendo concorrenza e innovazione. È fondamentale il coinvolgimento di tutti gli stakeholder, inclusi i rappresentanti del mercato e della società civile, per assicurare che dli standard tengano conto delle diverse esigenze e possano essere referenziati il più possibile direttamente, senza che la Commissione abbia necessità di introdurre ulteriori specifiche e procedure negli atti di esecuzione, al fine di promuovere l'accettazione e l'adozione diffusa dei portafogli di identità digitale nei servizi.

La tabella che segue riassume gli atti da emettere entro il 21 novembre 2024.

Articolo che richiede l'atto d'esecuzione	**Argomento dell'atto di esecuzione**	**Oggetto dell'atto d'esecuzione**
Articolo 5 bis, paragrafo 23	Requisiti, standard, specifiche e procedure per l'implementazione dei portafogli di identità digitale europei	Articolo 5 bis, paragrafi 4, 5, 8 e 18
Articolo 5 bis, paragrafo 24	Requisiti, standard, specifiche e procedure per l'onboarding degli utenti nel portafoglio europeo di identità digitale tramite mezzi di identificazione elettronica	Articolo 5 bis(24)
Articolo 5 ter, paragrafo 11	Specifiche e procedure per i requisiti dei soggetti che fanno affidamento sui portafogli di identità digitale europei	Articolo 5 ter, paragrafi 2, 5, 6, 7, 8 e 9
Articolo 5 quater, paragrafo 6	Standard, specifiche e procedure per la certificazione dei portafogli di identità digitale europei	Articolo 5 quater, paragrafi 1, 2 e 3
Articolo 5 quinquies, paragrafo 7	Formati e procedure per la pubblicazione di informazioni sui portafogli di identità digitale europei certificati	Articolo 5 quinquies, paragrafi 1, 4 e 5

Articolo 5 sexies, paragrafo 5	Standard, specifiche e procedure per le misure in caso di violazione della sicurezza dei portafogli di identità digitale europei	Articolo 5 sexies, paragrafi 1, 2 e 3
Articolo 11 bis, paragrafo 3	Standard, specifiche e procedure per l'abbinamento univoco dell'identità per le persone fisiche	Articolo 11 bis, paragrafo 1
Articolo 12, paragrafo 7	Disposizioni procedurali per la revisione tra pari degli schemi di identificazione elettronica	Articolo 12, paragrafo 5
Articolo 45 quinquies, paragrafo 5	Standard, specifiche e procedure per le attestazioni elettroniche di attributi qualificate	Allegato V
Articolo 45 sexies, paragrafo 2	Standard, specifiche e procedure per il catalogo degli attributi e per gli schemi di attestazione e verifica degli attributi	Articolo 45 sexies, paragrafo 1
Articolo 45 septies, paragrafo 6	Standard, specifiche e procedure per le attestazioni elettroniche di attributi rilasciate da o per conto di un organismo del settore pubblico	Articolo 45 septies, paragrafo 1
Articolo 45 septies, paragrafo 7	Standard, specifiche e procedure per la notifica degli organismi del settore pubblico che rilasciano attestazioni elettroniche di attributi	Articolo 45 septies, paragrafo 4
Articolo 46 bis, paragrafo 7	Formati e procedure per la relazione sulle attività degli organismi di vigilanza dei portafogli di identità digitale europei	Articolo 46 bis, paragrafo 7

Le modifiche introdotte col recepimento della direttiva NIS2

La Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (NIS2), adottata nel novembre 2022, abroga l'articolo 19 del regolamento eIDAS2 a partire dal 17 ottobre 2024, data in cui scatta l'obbligo di recepimento e di poco antecedente agli atti d'esecuzione di eIDAS2 da emettere entro il 21 novembre 2024.

L'articolo 19 di eIDAS2 riguarda la sicurezza dei servizi fiduciari, stabilendo i requisiti per la valutazione dei rischi, le misure di sicurezza e la notifica degli incidenti da parte dei prestatori di servizi fiduciari qualificati e non qualificati.

L'abrogazione dell'articolo 19 di eIDAS da parte della direttiva NIS2, che viene in pratica sostituito dall'articolo 21 della stessa, ha l'obiettivo di evitare duplicazioni e sovrapposizioni normative, in quanto la direttiva NIS2 introduce un quadro più ampio e aggiornato per la gestione della sicurezza informatica, che si applica anche ai prestatori di servizi fiduciari in quanto rientrano nella categoria dei soggetti essenziali o importanti definiti dalla direttiva.

Tuttavia, l'abrogazione dell'articolo 19 di eIDAS potrebbe avere un impatto significativo sul quadro normativo per i servizi fiduciari, in quanto le disposizioni specifiche relative alla sicurezza di tali servizi non saranno più direttamente incluse nel regolamento eIDAS2. Ciò potrebbe comportare una minore chiarezza e coerenza nella regolamentazione dei servizi fiduciari, con potenziali differenze nell'interpretazione e nell'applicazione delle norme di sicurezza tra i diversi Stati membri.

Per mitigare questi rischi dal direttiva NIS2 prevede l'emissione da parte della Commissione di appositi atti d'esecuzione in relazione all'applicazione dell'articolo 21 per i vari tipi di servizi nel perimetro della direttiva, inclusi i servizi fiduciari, e che per quanto possibile tali atti si dovranno basare su standard europei ed internazionali. Per questo motivo l'ETSI, ente di standardizzazione maggiormente coinvolto nell'emissione degli standard a supporto dei servizi fiduciari, ha proceduto alla revisione dello standard europeo EN 319 401. La revisione si concluderà con la pubblicazione presumibilmente entro giugno/luglio 2024 della nuova versione dello standard aggiornata ai requisiti NIS2 che, auspicabilmente, potrà essere tenuta in considerazione negli atti di esecuzione da emettere, per garantire una maggiore uniformità nel rispetto dei requisiti NIS2 nell'ambito dei servizi fiduciari.

Inoltre sarà importante garantire il coordinamento tra le autorità competenti per l'attuazione della direttiva NIS2 e quelle responsabili per la vigilanza sui servizi fiduciari ai sensi di eIDAS2, al fine di assicurare un approccio coerente e armonizzato alla sicurezza dei servizi fiduciari. In Italia l'ente di vigilanza è l'AGID mentre è previsto che l'ACN sarà l'autorità competente ai fini della NIS2. Per questo motivo la legge di delegazione europea 2022-2023 (21 febbraio 2024, n. 15) delega il Governo sia al recepimento della direttiva NIS2 che allo stabilire i ruoli di AGID ed ACN in relazione al regolamento eIDAS.

Gli atti di esecuzione da emanare entro il 21 maggio 2025 (12 mesi dall'entrata in vigore)

Per i servizi fiduciari ulteriori rispetto a quelli di emissione delle attestazioni elettroniche di attributo eIDAS2 prevede l'adozione di atti di esecuzione da parte della Commissione europea entro il 21 maggio 2025, a 12 mesi dall'entrata in vigore del Regolamento, con l'obiettivo di definire standard, specifiche e procedure per ogni tipo di servizio fiduciario qualificato, oltre a quanto previsto per i servizi non

qualificati nel già citato articolo 19 bis in relazione ai requisiti di cui all'Art. 19 bis, paragrafo 1, lettera a), che riguardano le misure per la gestione dei rischi legati alla fornitura di tali servizi.

Per i servizi fiduciari qualificati, diversi atti di esecuzione sono previsti entro 12 mesi, tra cui quelli relativi a standard, specifiche e procedure per l'accreditamento degli organismi di valutazione della conformità e per la relazione di valutazione della conformità (Articolo 20, paragrafo 4), per i requisiti per la verifica dell'identità e dei relativi attributi (Articolo 24, paragrafo 1 quater), per i requisiti per i prestatori di servizi fiduciari qualificati (Articolo 24, paragrafo 5), e per i requisiti per specifici servizi fiduciari, come ad esempio il nuovo servizio di gestione dei dispositivi di creazione di firme elettroniche qualificate a distanza (Articolo 29 bis, paragrafo 2), la convalida delle firme elettroniche qualificate (Articolo 33, paragrafo 2), la conservazione delle firme elettroniche qualificate (Articolo 34, paragrafo 2), i servizi di recapito elettronico certificato (Articolo 44, paragrafo 2) e i nuovi servizi di archiviazione elettronica (Articolo 45 undecies, paragrafo 2) e i registri elettronici (Articolo 45 terdecies, paragrafo 3).

La tabella seguente comprende un quadro completo di tali atti d'esecuzione.

Articolo che richiede l'atto d'esecuzione	**Argomento dell'atto di esecuzione**	**Oggetto dell'atto d'esecuzione**
Articolo 19 bis, paragrafo 2	Standard, specifiche e procedure per i requisiti dei prestatori di servizi fiduciari non qualificati	Articolo 19 bis, paragrafo 1, lettera a)
Articolo 20, paragrafo 4	Standard, specifiche e procedure per l'accreditamento degli organismi di valutazione della conformità e per la relazione di valutazione della conformità	Articolo 20, paragrafi 1 e 2
Articolo 21, paragrafo 4	Formati e procedure per l'avvio di un servizio fiduciario qualificato	Articolo 21, paragrafi 1 e 2
Articolo 24, paragrafo 1 quater	Standard, specifiche e procedure per la verifica dell'identità e degli attributi	Articolo 24, paragrafi 1, 1 bis e 1 ter
Articolo 24, paragrafo 5	Standard, specifiche e procedure per i requisiti dei prestatori di servizi fiduciari qualificati	Articolo 24, paragrafo 2
Articolo 29 bis, paragrafo 2	Standard, specifiche e procedure per i requisiti di un servizio qualificato di gestione dei dispositivi di creazione di firme elettroniche qualificate a distanza	Articolo 29 bis, paragrafo 1
Articolo 32, paragrafo 3	Standard per la convalida delle firme elettroniche qualificate	Articolo 32, paragrafo 1

Articolo 32 bis, paragrafo 3	Standard, specifiche e procedure per la convalida delle firme elettroniche avanzate basate su certificati qualificati	Articolo 32 bis, paragrafo 1
Articolo 33, paragrafo 2	Standard, specifiche e procedure per il servizio di convalida qualificato per le firme elettroniche qualificate	Articolo 33, paragrafo 1
Articolo 34, paragrafo 2	Standard, specifiche e procedure per il servizio di conservazione qualificato per le firme elettroniche qualificate	Articolo 34, paragrafo 1
Articolo 38, paragrafo 6	Standard, specifiche e procedure per i certificati qualificati di sigillo elettronico	Allegato III
Articolo 42, paragrafo 2	Standard per i requisiti delle validazioni temporali elettroniche qualificate	Articolo 42, paragrafo 1
Articolo 44, paragrafo 2	Standard per i requisiti dei servizi elettronici di recapito certificato qualificati	Articolo 44, paragrafo 1
Articolo 45, paragrafo 2	Standard per i requisiti dei certificati qualificati di autenticazione di siti web	Allegato IV
Articolo 45 undecies, paragrafo 2	Standard, specifiche e procedure per i servizi di archiviazione elettronica qualificati	Articolo 45 undecies, paragrafo 1
Articolo 45 terdecies, paragrafo 3	Standard, specifiche e procedure per i requisiti dei registri elettronici qualificati	Articolo 45 terdecies, paragrafo 1
Articolo 46 ter, paragrafo 7	Orientamenti sull'esercizio delle funzioni degli organismi di vigilanza e formati e procedure per la relazione sulle loro attività	Articolo 46 ter, paragrafi 4 e 6

L'adozione di questi atti di esecuzione sarà fondamentale per garantire un quadro normativo armonizzato e aggiornato per la sicurezza, l'affidabilità e l'interoperabilità dei servizi fiduciari nell'Unione. L'individuazione di standard e specifiche comuni promuoverà la competizione e contribuirà a rafforzare la fiducia degli utenti e a favorire l'adozione di soluzioni digitali avanzate in diversi settori.

Il ruolo centrale degli standard, in considerazione della complessità tecnica delle materie oggetto degli atti di esecuzione, è uno strumento essenziale per garantire un'ampia consultazione con gli stakeholder del settore, inclusi i prestatori di servizi fiduciari, le organizzazioni di standardizzazione, le autorità di vigilanza e i rappresentanti di utenti e PMI, per garantire che gli standard e le specifiche adottati siano effettivamente in grado di rispondere agli obbiettivi ambiziosi del Regolamento.

Conclusioni

eIDAS2 segna un'evoluzione significativa nel ruolo degli standard per l'identificazione elettronica e i servizi fiduciari nell'Unione europea ed è in linea con l'approccio generale adottato nei vari provvedimenti che sono stati recentemente introdotti o che sono in fase di adozione: si pensi ad esempio ai regolamenti sull'Intelligenza artificiale e sui Dati. L'adozione di un approccio più sistematico e armonizzato, basato su elenchi di standard di riferimento e la presunzione di conformità derivante dall'uso degli standard, contribuirà a rafforzare la fiducia, la sicurezza e l'interoperabilità nel mercato unico digitale europeo.

L'aggiornamento del Regolamento eIDAS rappresenta da una parte un passo importante verso la creazione di un'identità digitale europea affidabile, interoperabile e di utilizzo comune da parte dei cittadini europei, e, dall'altra, la creazione di un mercato unico europeo per tutti i servizi fiduciari. In tutto questo gli standard svolgono un ruolo chiave non solo nel loro ruolo più tradizionale di garantire ripetibilità ed interoperabilità tecnica, ma anche per garantire la fiducia, la sicurezza e la privacy dei cittadini e delle imprese nell'interazione con i servizi digitali pubblici e privati.

Il presidio delle attività degli enti di standardizzazione è essenziale sia per garantire che l'attuazione delle politiche governative in ambito digitale sia in linea con le decisioni tecniche prese sui tavoli europei, sia per gli operatori, affinché siano in grado di competere e cogliere le opportunità del mercato unico europeo, e non di subirlo.

N. 4 - 2024 - pp. 81-87

European Digital Identity Wallet: Impatti su Privacy e Sicurezza

Marco Mangiulli

Abstract [IT]: La più grande novità del regolamento 2024/1183 (eIDAS 2.0) è costituita dall'introduzione dello European Digital Identity Wallet, definito come un mezzo di identificazione elettronica che consentirà all'utente di conservare dati di identità, credenziali e attributi collegati all'identità, fornire tali dati su richiesta alle controparti al fine di effettuare autenticazione online e offline e dimostrare il possesso di attributi, nonché di creare firme elettroniche qualificate e sigilli elettronici qualificati. Nonostante il Wallet sia basato su paradigmi e modelli di identità digitale (quali ad esempio Self-Sovereign Identity, Zero Knowledge Proof, Selective Disclosure) che mettono al centro gli utenti, consentendogli di avere il pieno controllo sulla propria identità e sui dati ad essa connessi, è importante analizzare i diversi rischi, in termini di privacy e sicurezza, legati alla sua adozione.

Abstract [EN]: The biggest innovation of the Regulation 2024/1183 (eIDAS 2.0) is the introduction of the European Digital Identity Wallet, a mean of electronic identification that will allow its owner to secure store, manage, and share personal identification data, credentials and other attributes, as well as to create qualified electronic signatures and qualified electronic seals. Although the Wallet will be based on cryptographic schemes and trust models (such as Self-Sovereign Identity, Zero Knowledge Proof and Selective Disclosure) which allow users to have full control over their identity and attributes, it is important to analyse different risks related to its adoption, in terms of privacy and security.

Parole chiave: Digital Identity Wallet, identità digitale, eIDAS 2.0, zero knowledge proof, modello di trust

Sommario: 1. Il Wallet Europeo dell'Identità Digitale – 2. Il nuovo modello di trust – 3. Selective disclosure, ZKP e unlinkability – 4. Il regolamento eIDAS 2.0 – 5. I rischi – 6. Conclusioni

1. Il Wallet Europeo dell'Identità Digitale

Il portafoglio europeo dell'identità digitale rappresenta una grande novità nel panorama dei servizi fiduciari e della gestione dell'identità digitale.

La prima versione del regolamento eIDAS aveva svolto un ottimo lavoro per quanto riguarda i servizi fiduciari più tradizionali come ad esempio la firma elettronica e la validazione temporale. Sull'identità digitale invece, l'aver lasciato troppa autonomia agli stati membri ha comportato un'eccessiva frammentazione delle soluzioni adottate, ostacolando nei fatti la diffusione e l'interoperabilità dei servizi a livello transfrontaliero, nonostante il tentativo di porvi rimedio tramite la creazione dei "nodi eIDAS".

È proprio partendo da queste evidenze che nel giugno del 2021 la Commissione Europea ha proposto la revisione del regolamento eIDAS e la creazione di un portafoglio europeo per l'identità digitale, con l'obiettivo di avere una maggiore diffusione dell'identità digitale e un sistema davvero interoperabile.

Il Digital Identity Wallet è stato concepito con l'ambizione di non essere un semplice strumento di identificazione online, ma un "portafoglio" all'interno del quale far confluire dati di identificazione personale, credenziali e attributi verificabili. Ogni stato membro sarà obbligato a notificare almeno un'implementazione del Wallet, e questa dovrà essere conforme agli standard di riferimento in modo da fornire un'interfaccia comune verso gli utenti per l'autenticazione e la fruizione dei servizi.

2. Il nuovo modello di trust

Gli schemi di identità digitale fin qui implementati (si pensi ad esempio allo SPID italiano), sono basati sul modello dell'identità federata: al centro di questo modello si trova l'Identity Provider, che rilascia gli attributi agli utenti e decide quali sono i Service Provider con i quali tali attributi possono essere condivisi (previa autenticazione e autorizzazione da parte dell'utente). Nel modello basato sull' identità federata, l'Identity Provider "conosce" tutti i Service Provider "visitati" da uno specifico utente.

Il Digital Identity Wallet adotta invece il modello delle Verifiable Credentials, che mette al centro dell'ecosistema il soggetto titolare dell'identità, il quale ha il pieno controllo dei propri attributi e decide con chi condividerli (SSI - Self Sovereign Identity). In questo modello sono previsti tre attori fondamentali:

- Issuer: emette gli attributi (identificativi o di altre tipologie) tramite "attestazioni" opponibili a terzi e li rende disponibili all'Holder;
- Holder: gestisce gli attributi, conservandoli all'interno di un proprio "portafoglio", e decide di utilizzarli "presentandoli" ad un Verifier;
- Verifier: verifica le attestazioni di attributi presentate dall'Holder, ad

esempio al fine di concedere l'accesso ad un servizio.

Il modello delle Verifiable Credentials si basa sul cosiddetto "triangolo del trust": l'Issuer si fida dell'Holder, l'Holder si fida del Verifier e il Verifier si fida dell'Issuer.

A differenza del modello dell'identità federata, il modello delle Verifiable Credentials è un modello decentralizzato, in quanto chi emette gli attributi non ha successivamente nessun controllo sul loro utilizzo. L'Holder ha idealmente il controllo assoluto della propria privacy.

3. Selective disclosure, ZKP e unlinkability

Per comprendere a pieno i principi del nuovo modello di identità digitale, è opportuno introdurre alcune definizioni:

- **selective disclosure:** è la possibilità, offerta all'utente da una soluzione EUDI Wallet, di presentare un subset degli attributi emessi da un Issuer. Ad esempio uno studente ha bisogno di dimostrare di essere iscritto ad un'università per accedere ad una biblioteca: tramite il meccanismo della selective disclosure può dimostrare di essere iscritto all'università senza rivelare altre informazioni quali nome, cognome, numero di matricola ecc.
- **Zero-Knowledge Proof (ZKP):** metodo tramite il quale l'utente può provare ad una Relying Party (Verifier) che una certa "affermazione" è vera, senza fornire ulteriori elementi a parte l'affermazione stessa. Ad esempio un utente ha bisogno di dimostrare ad un istituto finanziario che è "solvente" senza condividere dettagli circa la sua storia finanziaria: tramite ZKP può dimostrare di non essere mai stato inadempiente su un prestito senza condividere informazioni finanziarie di dettaglio.
- **unlinkability:** mancanza delle informazioni necessarie per connettere ulteriori attributi a quelli forniti in maniera selettiva (selective disclosure) da un utente. Ad esempio: un utente ha fornito l'attributo relativo al suo nome ad una Relying Party, e quello relativo al suo cognome ad un'altra Relying Party. Le due Relying Party non possono scambiare alcuna informazione che consenta loro di associare la "divulgazione" (disclosure) del nome a quella del cognome.

4. Il regolamento eIDAS 2.0

Passiamo ora all'analisi delle principali indicazioni fornite dal nuovo regolamento eIDAS circa gli aspetti legati alla sicurezza e alla privacy del Wallet.

Una soluzione di EUDI Wallet deve consentire agli utenti di:

- richiedere, ottenere, selezionare, combinare, memorizzare ed eliminare, sotto l'esclusivo controllo dell'utente, dati identificativi personali e attributi elettronici;
- autenticarsi con una Relying Party online ed eventualmente offline, al fine di ottenere accesso a servizi pubblici e privati, garantendo la possibilità di effettuare la selective disclosure dei dati;
- validare e condividere, in modo sicuro, dati identificativi e attributi con un altro Wallet;
- generare pseudonimi e memorizzarli localmente in maniera cifrata;
- accedere ai log di tutte le transazioni effettuate con le diverse Relying Party tramite una dashboard. La dashboard deve consentire in maniera agevole di visualizzare le interazioni con le diverse Relying Party e i relativi dati scambiati, chiedere la cancellazione di tali dati ed eventualmente segnalare alle autorità privacy nazionali presunte violazioni;
- effettuare firme elettroniche qualificate o sigilli elettronici qualificati;
- esercitare il diritto alla portabilità dei dati;
- validare l'identità delle Relying Party;
- garantire il livello di assurance "high" nelle operazioni di identificazione e autenticazione;
- garantire la "revoca" di una specifica istanza del Wallet in caso di richiesta esplicita dell'utente, compromissione, cessazioni di attività di una Persona Giuridica ecc.

Gli utenti devono avere pieno controllo dell'EUDI Wallet e dei dati in esso contenuti. I provider di soluzioni EUDI Wallet non devono in nessun modo tracciare e collezionare informazioni circa l'utilizzo del Wallet che non siano strettamente necessarie per la fornitura stessa del servizio.

Allo stesso modo, i provider di dati identificativi personali o di attestazioni di attributi non devono, senza il consenso dell'utente, tracciare, linkare o correlare i dati relativi alle transazioni effettuate.

5. I rischi

Il modello di trust fin qui descritto e le prescrizioni del nuovo Regolamento eIDAS sembrano delineare uno scenario che mette al centro sicurezza, privacy ed interoperabilità.

Esistono tuttavia una serie di aspetti da tenere in considerazione.

In primo luogo sono tanti i ruoli previsti dall'ecosistema EUDI Wallet. Si riporta di seguito l'elenco contenuto all'interno dell'ARF (Architecture and Reference

Framework)[1]:

- EUDI Wallet Providers;
- Person Identification Data Providers;
- Qualified Electronic Attestation of Attributes (QEAA) providers;
- Qualified certificate for electronic signature/seal (QC) providers;
- Relying Parties;
- Non-qualified Electronic Attestation of Attributes (EAA) providers;
- Non-qualified certificate for electronic signature/seal providers;
- Providers of other Trust Services;
- Catalogues of attributes and schemes for the attestations of attribute providers.

Tutte queste entità dovranno essere "verificate" e "registrate" tramite un sistema che consenta di mantenere un elevato livello di trust. Il modello di "fiducia" identificato al momento sembra essere quello delle Trusted List, ma non esistono ancora specifiche definitive su come tale modello sarà implementato. Il modello "tradizionale" di pubblicazione e gestione delle Trusted List (liste in formato XML messe a disposizione tramite protocollo http(s) da parte di ciascuno degli stati membri) sembra non essere sufficientemente scalabile in un contesto di utilizzo come quello del Wallet. Tra le alternative più interessanti c'è quella che prevede l'utilizzo del modello EBSI[2] (European Blockchain Services Infrastructure) Trusted Issuers List. Altra alternativa altrettanto interessante è quella dell'OpenID Federation 1.0[3] (attualmente in stato *draft* come altri protocolli e specifiche di riferimento del Wallet), che ad oggi risulta essere il modello scelto per l'implementazione dell'Italian EUDI Wallet[4]. In ogni caso, indipendentemente dalle scelte implementative, risulta chiaro come la corretta gestione degli elenchi di fiducia sia un fattore determinante per la sicurezza dell'intero ecosistema. Una vulnerabilità nella gestione del trust avrebbe effetti devastanti: pensiamo ad esempio a cosa succederebbe se un attore malevolo riuscisse ad impersonare un Issuer di dati identificativi personali e/o di attributi.

Un altro aspetto da tenere in considerazione è quello relativo alla disponibilità di una dashboard tramite la quale l'utente potrà accedere per visualizzare tutte le transazioni effettuate tramite il Wallet, chiedere alle Relying Party la cancellazione dei dati scambiati e segnalare eventuali presunte violazioni all'autorità competente. Il vincolo imposto da eIDAS ai fornitori di Wallet obbliga questi ultimi a non raccogliere informazioni che non siano strettamente necessarie all'erogazione del servizio: c'è da chiedersi se le informazioni sulle transazioni effettuate dall'utente tramite Wallet siano davvero essenziali per erogare il servizio, se queste debbano essere mantenute sul device o essere trasferite verso i servizi di back-end del Wallet,

---

[1] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases/download/v1.3.0/ARF-v1.3.0-for-publication.pdf

[2] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[3] https://openid.net/specs/openid-federation-1_0.html

[4] https://italia.github.io/eudi-wallet-it-docs/versione-corrente/en/

e come debbano essere opportunamente protette in modo da non ricadere nel modello dell'Identity Provider e dell'identità federata (*Identity Provider* che "conosce" tutti i *Service Provider* visitati dal titolare dell'identità). Anche in questo caso una valida alternativa potrebbe essere quella dell'utilizzo di registri distribuiti (ad esempio tramite la *European Blockchain Services Infrastructure*), che comunque richiede di tenere in forte considerazione le tematiche relative alla privacy degli utenti.

Parlando di sicurezza, non possiamo non evidenziare il fatto che il Wallet verrà realizzato tramite app mobile, che dovranno interagire con delle API per le comunicazioni online e con altri dispositivi per quelle offline. È fondamentale tenere in conto, nella progettazione delle soluzioni, tutti i rischi legati al mondo delle applicazioni mobile (con particolare attenzione alle misure per prevenire l'esportazione di chiavi crittografiche), delle API e dei protocolli di comunicazione a corto raggio.

Per quanto riguarda selective disclosure, ZKP e unlinkability, sono molti gli aspetti da tenere in considerazione. L'ETSI Technical Report 119 476 v 1.1.1[5] contiene un'analisi completa e una serie di raccomandazioni su questi temi in relazione ai formati più rilevanti previsti dall'EUDI Wallet per i dati identificativi personali e per gli attributi: ISO mobile driving license[6] e W3C Verifiable Credentials[7] (insieme a SD-JWT [8]).

Un'ultima riflessione sul tema dell'interoperabilità: se da un lato dovrà esserci obbligatoriamente un portafoglio "pubblico" per ogni Stato Membro, la cui interoperabilità dovrà essere garantita dal regolamento eIDAS, dall'ARF e dagli ulteriori standard tecnici che seguiranno, dall'altra è molto probabile che ci saranno una serie di soluzioni "private". L'auspicio è che anche tali soluzioni siano basate su standard comuni ed interoperabili, e che non siano invece delle soluzioni "verticali" limitate all'utilizzo di specifici servizi.

6. Conclusioni

L'avvento del Digital Identity Wallet rappresenta un'enorme opportunità per la diffusione dell'identità digitale all'interno dell'Unione Europea e per il superamento dei problemi di interoperabilità che affliggono gli attuali schemi di identificazione notificati dai vari stati membri.

L'adozione di modelli e paradigmi che consentono di restituire agli utenti il pieno controllo sulla propria identità e sui dati ad essa connessi rappresentano inoltre un deciso passo in avanti in termini di privacy e sicurezza.

---

5 https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.01.01_60/tr_119476v010101p.pdf

6 ISO/IEC 18013-5 (ISO mDL)

7 Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022 - Verifiable Credentials Data Model v2.0 W3C Candidate Recommendation Draft 27 February 2024

8 https://www.ietf.org/archive/id/draft-fett-oauth-selective-disclosure-jwt-02.html

È tuttavia fondamentale che nella definizione di framework e specifiche tecniche, nonché nella progettazione e nella realizzazione delle soluzioni, vengano adottate tutte le misure necessarie per realizzare un ecosistema davvero sicuro e in grado di tutelare la privacy dei cittadini.

Una menzione finale al tema dell'interoperabilità: il successo e la diffusione del Wallet passa dalla capacità di realizzare un ecosistema davvero interoperabile ed utilizzabile all'interno dei vari stati membri. È necessario che sui temi dell'interoperabilità non si accettino compromessi e si mettano al centro gli interessi comuni rispetto a quelli dei singoli stati.

N. 4 - 2024 - pp. 88-92

L'interoperabilità del Portafoglio d'Identità Europeo

Andrea De Maria

Abstract [IT]: Il Portafoglio Europeo di Identità Digitale è un progetto ambizioso e complesso, che deve considerare sia requisiti di interoperabilità che di sicurezza, assieme alle specificità presenti nei differenti Stati Membri. Lo strumento utilizzato per guidare l'implementazione delle differenti soluzioni nazionali è l'ARF – Architecture Reference Framework, un documento vivo dove vengono definiti formati dei dati, protocolli e processi. Molto lavoro è stato fatto, molto lavoro ancora rimane da fare.

Abstract [EN]: The European Digital Identity Wallet is an ambitious and complex project, where interoperability, security and national requirements have to be taken into account. The main tool used to guide the implementation of the different national solutions is the ARF – Architecture Reference Framework, a living document where protocols, data formats and processes are outlined. A lot has been done; a lot has to be done.

Parole chiave: ARF, Wallet, EUDI, Interoperability

Sommario: 1. La sfida; 2. Approccio Iterativo; 3. ARF – Versione attuale; 4. Cosa è ancora da fare; 5. Conclusioni

1. La sfida

È conosciuto come *Wallet*, o *EUDI Wallet*, o *Wallet europeo di identità digitale*, o *Portafoglio Europeo di Identità Digitale*. È un progetto ambizioso e complesso che coinvolge diversi Stati Membri. La sfida è partita il 3 giugno 2021 con la pubblicazione della raccomandazione 946/2021 che chiedeva agli Stati Membri di lavorare allo sviluppo di un'architettura e di un quadro di riferimento per l'identità digitale in Europa.

La Raccomandazione chiedeva di utilizzare l'Expert Group eIDAS, che ha pubblicato nel febbraio 2022 il primo Outline dell'Architecture and Reference Framework (ARF). Il documento delinea un sistema di identità digitale ispirato ai principi della Self Sovereign Identity pur senza adottarli esplicitamente, in cui identità digitale e attributi dell'identità (patente di guida, ad esempio) possono essere utilizzati sia in servizi online che in transazioni effettuate di persona, nel mondo fisico. Vengono

ipotizzati diversi casi d'uso e una prima architettura, in cui vengono evidenziati ruoli e interfacce. Al centro c'è il Wallet, inteso come applicazione per smartphone in cui vengono caricati gli attributi e i dati di identificazione (PID – Personal Identification Data).

Lo schema proposto è infatti completamente diverso dagli schemi di identità federata a cui siamo abituati, in cui i dati di identità necessari a un Service Provider (fornitore di servizio - il servizio anagrafe online di un comune, ad esempio) vengono forniti da un Identity Provider (fornitore di identità – i vari provider SPID o il Ministero dell'Interno, per la CIE) a cui il Service Provider si collega.

Stavolta i dati di identità vengono caricati direttamente nel Wallet al momento della sua attivazione e vengono forniti dal cittadino al Service Provider direttamente, senza che quest'ultimo debba contattare un Identity Provider. In questo modo l'Identity Provider non sa più su quale servizio il cittadino sta facendo accesso.

Questo schema riprende i modelli di identità decentralizzata, su cui si sta lavorando da tempo. Gli esperti sono generalmente d'accordo sull'utilità e sulla fattibilità dei modelli di identità decentralizzata (o sovereign) ma i principi che stanno alla loro base non sono stati ancora applicati su una scala comparabile a quella attesa per il Wallet europeo.

Il problema principale che si pone per un sistema che deve essere valido in tutta Europa è l'interoperabilità.

Non è affatto semplice assicurare l'interoperabilità in un ecosistema che dovrà comprendere Wallet pubblici e privati, servizi pubblici e privati, dati provenienti da fonti autoritative e no; casi d'uso in cui i dati vengono presentati in interazioni faccia a faccia (inizialmente chiamate *offline* e ora *proximity*, per includere anche le interazioni che un utente può avere con un sistema automatico come un gate di frontiera) e casi d'uso in cui i dati vengono trasmessi a sistemi remoti a cui si accede da smartphone o da computer, il tutto tenendo conto di differenti indicazioni legislative nazionali che indicano come trattare i dati nei differenti casi d'uso, garantendo la sicurezza delle transazioni e la privacy dei cittadini (con un approccio Security by Design e Privacy by Design) e utilizzando un modello non ancora provato su larga scala.

2. Approccio Iterativo

Per affrontare tale complessità la Commissione (DG CONNECT) e l'Expert Group eIDAS hanno adottato un approccio iterativo, in cui l'ARF è un documento vivo, che viene pubblicato in versioni successive che partono dalla definizione del modello generale e dei casi d'uso per definire man mano le interfacce, i processi, i protocolli, l'architettura di trust, i data model.

L'ARF ha lo scopo di definire le specifiche necessarie per lo sviluppo di una soluzione di Wallet interoperabile. Oltre ai requisiti comuni di sicurezza, definirà

soprattutto le interfacce, dove queste potranno riguardare componenti gestite da stati differenti (es. Wallet italiano utilizzato per mostrare la patente di guida ad un verificatore francese) ma lascerà spazio per le specificità nazionali, come la modalità di ottenimento del PID o l'interfaccia tra le fonti di dati e i Provider.

L'ARF non è ancora un documento finalizzato, ma viene aggiornato di continuo dalla Commissione e dall'Expert Group e reso pubblico periodicamente.

L'evoluzione dell'ARF è legata allo sviluppo di una Reference Implementation, che verrà rilasciata in Open Source dalla Commissione per essere utilizzata nelle implementazioni nazionali, e ai Large Scale Pilots, progetti co-finanziati dalla Commissione a cui partecipano enti privati e pubblici di diversi Stati Membri. Sia la Reference Implementation che i Large Scale Pilots si basano sull'ARF e forniranno feedback per le versioni successive dell'ARF. In questo modo l'ARF potrà tener conto degli effettivi problemi implementativi e delle specificità nazionali, come l'interazione con schemi di identità nazionali notificati (SPID e CIE, per l'Italia) e si potrà verificare l'effettiva interoperabilità in scenari cross-border.

3. ARF – Versione attuale

La versione attuale è la 1.3, pubblicata a inizio marzo 2024, e non descrive ancora completamente tutti gli aspetti necessari alla completa implementazione di una soluzione. Molti aspetti però sono stati affrontati e definiti (con specifico riferimento ai due casi d'uso principali individuati: identificazione/autenticazione online e mobile Driving License); ne diamo qui una sintetica descrizione.

Ruoli

Gli attori del sistema sono tutti definiti. I principali:

- Provider – ricevono gli attributi dalle Authentic Source e li forniscono al Wallet in forma di attestazione. Uno speciale Provider è il PID Provider, che fornisce i dati di identificazione;
- Wallet Instance – la specifica istanza del Wallet su un dispositivo. Riceve le attestazioni dai Provider e le presenta sotto il controllo dell'utente ai Relaying Party;
- Relaying Party – ricevono dal Wallet le attestazioni, ne verificano l'autenticità e la validità al fine di erogare un servizio.

Modello di dati

Vengono definiti i formati dati generali per il PID e per le (Q)EAA – (Qualified) Electronic Attribute Attestation.

Per le (Q)EAA viene anche suggerito (SHOULD) il protocollo di emissione, OIDC4VCI, mentre l'emissione del PID verso il Wallet viene lasciata alle scelte nazionali.

La Selective Disclosure (possibilità di fornire solo una parte dei dati dell'attestazione) si ottiene utilizzando gli schemi SD-JWT (Selective Disclosure Jason Web Token) o Mobile Security Object, a seconda che PID o (Q)EAA vengano presentato a un servizio online o in una transazione fisica.

In sintesi i formati saranno:

Remote Flow:

- Data Model: W3C Verifiable Credential
- Codifica: JSON
- Selective Disclosure: SD-JWT

Proximity Flow:

- Data Model: ISO18013-5
- Codifica: CBOR
- Selective Disclosure: Mobile Security Object ISO 18013-5

Il formato dati di dettaglio viene fornito per il PID (formati W3CVC/JSON e ISO18013-5/CBOR) e per la mobile Driving License (solo formato ISO18013-5/CBOR per la presentazione in prossimità).

Modello di Trust

L'ARF introduce un modello di Trust mediante il quale ogni attore può assicurarsi dell'autenticità delle informazioni che gli vengono inviate.

Il modello di Trust deve rispondere, ad esempio, ai requisiti:

- un utente deve essere sicuro che l'app 'Wallet' che sta utilizzando sia autentica
- un utente deve essere sicuro che l'attestazione che riceve viene da un Provider autorizzato
- il Provider deve essere sicuro dell'identità dell'utente
- il Provider deve essere sicuro che l'app che ha chiesto l'attestazione sia un'app autorizzata
- il Relying Party deve essere sicuro del Provider di attestazione, dell'istanza di Wallet, dell'identità dell'utente.

Queste sono solo alcune delle relazioni di trust che possono essere assicurate anche mediante meccanismi crittografici (cryptographic binding). Il dettaglio dei meccanismi di binding deve ancora essere definito.

4. Cosa è ancora da fare

L'ARF vedrà sicuramente nuove versioni che dovranno definire diversi aspetti. I notevoli profili di novità del progetto fanno sì che ci si sia dovuti riferire a standard non ancora finalizzati. Diversi aspetti legati al ciclo di vita delle attestazioni vanno ancora chiariti, soprattutto relativi alla revoca, così come diversi ambiti di sicurezza e di trust.

Diversi casi d'uso sono ancora da esplorare e verranno definiti anche in base al feedback proveniente dai Large Scale Pilot. In particolare, il Wallet può essere il vettore delle Digital Travel Credential (DTC), versione digitale dei documenti di viaggio in fase di studio e sperimentazione in ambito ICAO; si potranno caricare sul Wallet le certificazioni professionali e i diplomi di studio, o le prescrizioni mediche.

Fuori dall'ARF vanno poi definiti gli aspetti di Governance. Il Wallet dovrà avere una certificazione funzionale e una certificazione di sicurezza. Sarà necessaria una certificazione anche per le componenti crittografiche della soluzione. Non sono ancora definiti gli schemi di certificazione da utilizzare per garantire un livello di sicurezza su cui tutti gli stati possano fare affidamento.

5. Conclusioni

Il progetto del Wallet Europeo di Identità Digitale è complesso e molto innovativo. L'approccio iterativo adottato, il contributo degli esperti europei e il feedback fornito dai Large Scale Pilot e dalla Reference Implementation dovranno far convergere l'ARF verso una specifica di interoperabilità adottabile da tutti gli Stati Membri. Molto lavoro è ancora necessario per finalizzare l'ARF, per definire gli standard tecnici e per mettere a punto e implementare tutte le regole di Governance che potranno rendere il Wallet un sistema davvero operativo.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 93-99

Il regolamento 2024/1183 (eIDAS 2.0): la sostenibilità come leva per una rapida diffusione

Andrea Sassetti

Abstract [IT]: Dal 2014 il Regolamento eIDAS rappresenta la disposizione comunitaria di riferimento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche.

Si attendeva da anni una sua revisione che ne colmasse alcune lacune e che potesse rispondere alle nuove sfide che i processi di digital transformation, la tecnologia e il mercato hanno introdotto negli ultimi anni. I nuovi servizi fiduciari definiti nel regolamento - quali il EUDI Wallet, gli attestati elettronici di attributi qualificati così come il nuovo servizio di conservazione digitale - e una forte spinta al tema dell'interoperabilità indicano chiaramente la strada che i prestatori di servizi fiduciari qualificati (QTSP) hanno difronte: confrontarsi sempre più con il mercato unico europeo per realizzare un vero "single digital market" diventando inevitabilmente un prestatore di servizi fiduciari a livello Europeo.

eIDAS 2.0 rappresenta quindi un'occasione imperdibile per creare valore per cittadini, aziende, professionisti e pubblica amministrazione ma che richiede di porre grande attenzione al tema della sostenibilità senza la quale l'intero ecosistema potrebbe non cogliere gli importanti obiettivi che il regolamento si è posto.

Abstract [EN]: Since 2014, the eIDAS Regulation has represented the reference regulation on electronic identification, trust services and electronic transactions.

A revision has been long awaited to fill a few gaps and to respond to the new challenges that the digital transformation processes, the evolution of technology and the market have introduced in recent years. The new trust services defined in the regulation - such as the EUDI Wallet, the electronic attestation of attributes as well as the new digital preservation service - and a strong push towards the issue of interoperability clearly indicate the path qualified trust service providers (QTSP) must follow: dealing with the single European market to create a true "single digital market", QTSPs are inevitably becoming European service providers instead of remaining on the national level. eIDAS 2.0, therefore, represents an unmistakeable opportunity to create value for citizens, companies, professionals and public administration. In the same time, we need to raise the issue of sustainability. Without sustainable op-

erational and business models, the entire ecosystem may not be able to achieve the important objectives that the regulation itself has set.

Parole chiave: eIDAS, servizi fiduciari, wallet, attestati elettronici di attributi, interoperabilità, sostenibilità

Sommario: 1. Il nuovo regolamento eIDAS - 2. I nuovi servizi fiduciari - 3. I Trust Service come servizi abilitatori alla Digital Economy - 4. Il concetto di European QTSP - 5. L'interoperabilità come valore aggiunto per il single digital market - 6. La sostenibilità come elemento chiave per la diffusione dei servizi trust del EUDI Wallet

1. Il nuovo regolamento eIDAS

Dal 2014 il Regolamento eIDAS rappresenta la disposizione comunitaria di riferimento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche.

Si attendeva da anni una sua revisione che ne colmasse alcune lacune e che potesse rispondere alle nuove sfide che i processi di digital transformation, la tecnologia e il mercato hanno introdotto negli ultimi anni. I nuovi servizi fiduciari definiti nel regolamento - quali il EUDI Wallet, gli attestati elettronici di attributi qualificati così come il nuovo servizio di conservazione digitale - e una forte spinta al tema dell'interoperabilità indicano chiaramente la strada che i prestatori di servizi fiduciari qualificati (QTSP) hanno di fronte: confrontarsi sempre più con il mercato unico europeo per realizzare un vero "single digital market" diventando inevitabilmente un prestatore di servizi fiduciari a livello europeo.

eIDAS 2.0 rappresenta quindi un'occasione imperdibile per creare valore per cittadini, aziende, professionisti e pubblica amministrazione ma che richiede di porre grande attenzione al tema della sostenibilità senza la quale l'intero ecosistema potrebbe non cogliere gli importanti obiettivi che il regolamento si è posto.

Questo traguardo legislativo rappresenta un passo fondamentale data anche l'importanza che regolamenti europei come questo hanno per le aziende che intendono operare sul mercato dell'Unione Europea in collaborazione con i governi degli Stati Membri.

Sebbene sarebbe stato opportuno un maggior coinvolgimento nell'ecosistema europeo da parte dei legislatori, i prestatori di servizi fiduciari rimangono comunque collaborativi e propositivi nei prossimi passaggi legislativi dove le istituzioni europee ed i rappresentanti dei governi degli Stati Membri si accingono a sviluppare gli atti implementanti. Questo perché riteniamo sia importante sottolineare come il settore dei fornitori di servizi fiduciari nell'Unione Europea (ed in Italia) sia all'avanguardia rispetto al resto del mondo con tante realtà europee (ed italiane) che hanno dimostrato di essere l'avanguardia tecnologica del settore e continuano ad essere interessate ad occupare quello spazio.

Il settore dei fornitori di servizi fiduciari è un ecosistema molto complesso e spesso, per i non addetti ai lavori, risulta difficile capire come questo possa esser regolamentato sebbene sia uno dei settori già particolarmente disciplinati. Il nuovo regolamento dovrebbe favorire la competizione dei fornitori in Stati Membri differenti, creando un ecosistema europeo a tutti gli effetti.

2. I nuovi servizi fiduciari

Il nuovo regolamento introduce nuovi servizi fiduciari tra cui il wallet digitale, l'attestazione elettronica di attributi e la conservazione digitale, mentre introduce alcuni aggiornamenti nell'impostazione dei servizi fiduciari già definiti in eIDAS quali la firma qualificata, l'e-delivery qualificato e l'autenticazione dei siti web.

L'European Digital Identity Wallet (EUDIW) rappresenta la più importante novità del nuovo regolamento eIDAS che lo introduce come l'evoluzione "de facto" della identità digitale, sia per un utilizzo online che offline.

Il Wallet gestirà la nostra identità digitale alla quale potranno essere associati, al suo interno, una o più attestazioni di attributo qualificato (quali, ad esempio, titoli di studio, poteri di rappresentanza, attestazioni in ambito di finanza digitale, etc.) e dove potremo anche gestire la versione digitale del documento d'identità e della patente di guida. Sempre sugli attestati elettronici di attributo, come per gli altri servizi fiduciari, anche loro potranno essere qualificati o non qualificati (ossia emessi da un prestatore di servizi qualificato o da altro soggetto) con una differenza sostanziale: gli attestati elettronici di attributi qualificati e quelli rilasciati da o per conto di un ente pubblico responsabile di una fonte autentica devono avere pari valenza giuridica di quelli rilasciati "su carta", mentre a quelli non qualificati non possono essere negati effetti giuridici per il solo fatto di essere emessi in forma elettronica

Ma non solo. Grazie alle funzionalità di creazione di firme e sigilli elettronici qualificati il wallet consentirà di svolgere molteplici attività, dal check-in in aeroporto al noleggio di un'automobile, dal presentare la dichiarazione dei redditi a iscriversi all'università fino a richiedere un prestito bancario con una procedura semplice, veloce e altamente sicura.

3. I Trust Service come servizi abilitatori alla Digital Economy

Nelle varie declinazioni della Digital Economy quali Intelligenza Artificiale, Metaverso, Internet of Things, Cybersecurity, Payment Service Directive, ed ulteriori, l'elemento dal quale non possiamo prescindere è la fiducia.

Aver fiducia nei servizi quotidianamente fruiti da aziende, professionisti e cit-

tadini è alla base delle azioni che compiamo nel mondo digitale.

Autenticità, integrità, riservatezza e non ripudio sono elementi cardine su cui basare un processo digitale, e questo viene garantito dai servizi fiduciari che rappresentano la tecnologia abilitante ai processi di dematerializzazione.

Quando parliamo di processi che trattano un numero elevato di dati, spesso anche sensibili, la digitalizzazione di questi diventa strategica. E nel momento che andiamo a portare in digitale processi pre-esistenti o a pensare a processi digital by-design l'autenticità, l'integrità, la riservatezza e il non ripudio dei documenti che vengono gestiti, firmati, trasmessi, conservati diventa elemento fondamentale per poter riporre fiducia nel processo che stiamo digitalizzando.

È quindi importante che sia a livello di Unione Europea che di singoli Stati Membri ci sia la consapevolezza che ogni qualvolta nelle specifiche normative, regolamenti ed atti si debbano garantire i principi sopra citati si possa, anzi si debba far riferimento ai servizi fiduciari come alla tecnologia in grado di garantire detti principi e, di conseguenza, la fiducia richiesta.

In tal senso, sin dalla presentazione della proposta di regolamento sul Framework dell'Identità Digitale Europea, la Commissione Europea ha insistito molto sul ruolo chiave che i servizi fiduciari, ed in particolar modo il Digital Identity wallet, avranno nel mercato unico europeo.

La scelta di puntare ad una larga diffusione dei servizi fiduciari nell'Unione Europea va letta anche nell'ottica di continuare a focalizzare l'attenzione sulla digitalizzazione delle Piccole e Medie Imprese (PMI) che sono la colonna vertebrale dell'UE.

La Commissione Europea ha investito molto negli anni passati per ridurre il più possibile tutti gli ostacoli che potessero favorire processi di digitalizzazione, sia per quanto riguarda la raccolta di dati che nell'utilizzo di procedure facilitate che non sfavorisse l'ecosistema di PMI che operano in UE.

In questi termini i servizi fiduciari, quali la firma qualificata, il recapito qualificato, la conservazione digitale e non ultimo il wallet sono visti dalle istituzioni europee come l'anello mancante nella costruzione di un vero e proprio mercato unico europeo.

Come sappiamo, l'Unione Europea si regge sulla libera circolazione di beni, servizi, capitali e persone all'interno dei suoi confini e, sebbene abbia ampi margini di miglioramento, il mercato unico europeo raccoglie quasi 450 milioni di consumatori e rappresenta il 18% del prodotto interno lordo mondiale.

Nonostante sia già ampiamente possibile per qualsiasi cittadino europeo spostarsi comodamente all'interno della UE, aprire una propria attività o commerciare, rimango ancora barriere che ne ostacolano e/o limitano l'accesso. In questa ottica, la Commissione Europea ritiene che l'adozione di procedure digitali che facciano uso dei servizi fiduciari sarà il primo passo per facilitare le procedure di supporto alle PMI ma sarà altrettanto semplice per i cittadini UE di usufruire di servizi intra-UE tramite l'uso di questi servizi, tra cui il Wallet.

Viste queste considerazioni, sarà ovviamente cruciale il ruolo che gli Stati Membri giocheranno nell'applicazione del Regolamento come anche nella decisione

da parte dei singoli stati di gestire la concorrenza all'interno del mercato nazionale nella tutela di cittadini ed imprese. Sotto questo aspetto, la Commissione Europea sembra interessata a voler continuare a vigilare il mercato assicurando una appropriata interpretazione del quadro normativo.

Va inoltre sottolineato che la Commissione Europea ha lavorato molto al nuovo regolamento eIDAS anche in previsione del ruolo fondamentale che il wallet e l'identità digitale potranno avere: il loro utilizzo nel metaverso.

Sappiamo che già che l'Unione Europea si è spesa molto nella costruzione di un quadro normativo che andasse a regolamentare l'Intelligenza Artificiale, valutandone il grado di rischio. A questo ambito, va aggiunto il crescente interesse della Commissione verso quello che viene definito il Metaverso o i Mondi Virtuali. La previsione si basa sulla convinzione che progressivamente cittadini ed imprese, grazie anche all'avvento di IA e altre tecnologie, avranno sempre più accesso ad un mondo virtuale dove potranno condurre la loro "vita digitale" in perfetta specularità con quella "offline".

Per questo motivo, sarà importante aver definito nei dettagli come certificare l'esistenza di una persona fisica all'interno di uno spazio virtuale per poterle permettere di svolgere il maggior numero di attività richieste.

4. Il concetto di European QTSP

La discussione sul regolamento eIDAS 2.0 ha portato alla luce un punto già evidente ai vari operatori del settore: l'Unione Europea è il mercato più sviluppato in termini di gestori di servizi fiduciari e con il maggior numero di aziende specializzate nell'implementazione di servizi e soluzioni che utilizzano i servizi fiduciari stessi e garantiscono il riconoscimento dell'identità digitale.

In sede di negoziazione del regolamento, questo punto ha permesso di segnalare al legislatore la presenza di un ecosistema di imprese che deve essere tutelato e che deve poter continuare a garantire servizi a pubbliche amministrazioni, aziende e ovviamente cittadini in tutta l'Unione Europea.

Per fare ciò, sarà necessario che la Commissione Europea e i rappresentanti degli Stati Membri definiscano degli atti implementativi che garantiscano la possibilità a tutti i gestori di servizi fiduciari di continuare ad investire nel settore ed in particolare a far si che questi investimenti siano rivolti non più al solo mercato nazionale ma che possano vedere una loro applicazione anche al mercato europeo.

Il regolamento eIDAS già nella sua prima stesura consentiva, in teoria, ad un fornitore di servizi fiduciari qualificati (Qualified Trust Service Provider – QTSP – come definito dal regolamento eIDAS) di offrire i propri servizi in tutti gli stati membri ma, di fatto, per molti di essi non venivano definite delle regole per l'interoperabilità che hanno limitato fortemente la realizzazione del single digital market come definito nel regolamento eIDAS.

Il nuovo regolamento eIDAS, invece, punta molto alla diffusione dei servizi fiduciari cross border e di conseguenza all'interoperabilità elevando, a pieno titolo, i QTSP a European QTSP.

Questo è indubbiamente un notevole passo avanti ed un'apertura ad un mercato più ampio per gli operatori del settore che però rischia di scontrarsi con una complessità legislativa consistente.

C'è il concreto rischio che ogni Stato Membro interpreti ed implementi in maniera differente il regolamento portando ad una evidente difficoltà nella gestione del mercato. Questo potrebbe portare a inutili disservizi a cittadini ed imprese anche se l'auspicio di tutti è che i legislatori siano in grado di rivedere le linee guida entro breve.

5. L'interoperabilità come valore aggiunto per il single digital market

L'interoperabilità è uno dei pilastri chiave di questo nuovo regolamento che altrimenti impedirebbe a cittadini ed imprese di muoversi autonomamente e senza ostacoli, usufruendo di numerosi servizi.

In tal senso, il wallet digitale ha alla base proprio il concetto di interoperabilità andando a renderlo ampiamente utilizzabile per identificarsi o dimostrare determinate informazioni personali, per poter accedere a servizi digitali pubblici e privati in tutta l'UE.

Con questo nuovo regolamento, le previsioni in tema di interoperabilità mirano a migliorare la connessione tra le diverse piattaforme e soluzioni di identità digitale, semplificando i processi di verifica dell'identità e aumentando l'efficienza delle transazioni digitali.

Anche nel contesto della archiviazione elettronica, la Commissione Europea ha, a più riprese, sottolineato come nella discussione con gli Stati Membri riguardo i requisiti nazionali ci sia un interesse condiviso a focalizzarsi su una regolamentazione il più possibile comune a tutti i Paesi Membri, soprattutto in un'ottica di interoperabilità.

Stesso principio viene applicato nel caso del recapito qualificato dove l'interoperabilità gioca un ruolo chiave dato che deve essere alla base del funzionamento di un servizio che garantisca un livello minimo di armonizzazione per incoraggiarne l'utilizzo e la diffusione.

L'interoperabilità torna ad essere protagonista anche nel caso dei certificati QWACs (Qualified Web Authentication Certificate) dove si va a richiedere a tutti i fornitori di siti web di garantire supporto e interoperabilità con i certificati qualificati per l'autenticazione dei siti web emessi in piena conformità con i requisiti del regolamento.

6. La sostenibilità come elemento chiave per la diffusione dei servizi trust del EUDI Wallet

C'è un ultimo elemento che è stato alla base delle fasi finali della discussione sul nuovo regolamento eIDAS: la gratuità dei servizi di firma e di wallet.

Facendo la dovuta premessa che il settore dei servizi fiduciari è un settore altamente tecnico e già, in grossa parte, regolamentato da disposizioni nazionali, internazionali e standard, rimane comunque un ecosistema dove rimane difficile per i non addetti ai lavori poter andare a definire i parametri legislativi entro cui i fornitori possono operare.

In tal senso, in sede di Parlamento Europeo, è stata introdotta in corso d'opera la proposta di mantenere i servizi completamente gratuiti. La proposta ha indubbiamente raccolto un generale interesse da parte della maggioranza degli interlocutori con il sincero interesse di non voler imporre al cittadino una spesa nell'accesso a determinati servizi.

Questa proposta ha però, di riflesso, generato preoccupazioni da parte degli operatori del settore perché, sebbene ci fosse una sincera condivisione della preoccupazione di non voler gravare sui cittadini, rischiava di crearsi un vulnus perché non veniva specificato chi avrebbe investito su tale servizio. Senza peraltro contare che, in una prima stesura, non veniva nemmeno chiarito il concetto di persona fisica che, per chi conosce la materia della firma digitale, avrebbe creato discrepanze nel capire se è un cittadino o un'impresa a richiedere una firma, così come la distinzione tra l'utilizzo personale o professionale della firma digitale stessa.

Il risultato finale del regolamento lascia ampio spazio di interpretazione agli Stati Membri riguardo alla sostenibilità dei servizi fiduciari e si attendono ulteriori linee guida da parte dei legislatori europei a tal proposito e ciò pone un tema cruciale per la reale diffusione di questi servizi così come definiti nel regolamento eIDAS.

Senza una visione di sostenibilità dell'intero sistema, difficilmente gli operatori investiranno sullo sviluppo e diffusione dei servizi fiduciari, con conseguenze a discapito anche della creazione del mercato unico europeo.

Rimane la speranza che questi atti implementativi tanto attesi permettano di far chiarezza in proposito dando così la possibilità alle tante realtà europee che forniscono servizi fiduciari di poter fare investimenti in tutta l'Unione Europea nel rispetto della concorrenza e del libero mercato.

N. 4 - 2024 - pp. 100-104

L'attestazione elettronica di attributi

Giovanni Manca

Abstract [IT]: Il rilascio di attestati elettronici di attributi è un nuovo servizio fiduciario stabilito nel nuovo regolamento europeo eIDAS. Questi attestati sono indispensabili per il corretto funzionamento del Portafoglio Europeo di Identità Digitale poiché specificano a quale titolo l'identità digitale del soggetto viene utilizzata nello specifico contesto operativo. Gli attributi possono essere di una persona fisica, giuridica o di un oggetto. Quest'ultimo aspetto amplia l'associazione degli attributi anche a elementi operativi come strutture meccaniche, sensori o elementi associabili all'*Internet of Things*. Una ulteriore caratteristica degli attestati elettronici di attributi è che possono essere utilizzati in tutta l'Unione con lo stesso valore giuridico.

Abstract [EN]: The issuing of electronic attestations of attributes is a new trust service established in the new European eIDAS regulation. These attestations are essential for correct operation of the European Digital Identity Wallet as they specify in what capacity the subject's digital identity is used in the specific operational context. Attributes can be of a natural person, legal entity or object. This last aspect extends the association of attributes also to operational elements such as mechanical structures, sensors or elements that can be associated with the Internet of Things. A further characteristic of electronic certificates of attributes is that they can be used throughout the Union with the same legal value.

Parole chiave: eIDAS, servizi fiduciari, attributi, attestati elettronici di attributi.

Sommario: 1. Le modifiche al testo del regolamento – 2. Le prospettive operative – 3. Conclusioni

1. Le modifiche al testo del regolamento

La centralità dell'attestazione elettronica degli attributi è strettamente collegata all'identità digitale. La stessa persona fisica o giuridica agisce in rete o fuori rete con le varie istanze possibili associate alla propria identità digitale che è, ovviamente, univocamente connessa alla persona fisica. A quest'ultima si associano gli attestati elettronici degli attributi. Questi possono essere qualifiche accademiche, compresi diplomi universitari o altri titoli di studio, qualifiche professionali o personali come la patente di guida. La loro peculiarità è che sono legalmente riconosciuti in tutta

l'Unione, le pubbliche amministrazioni ne beneficiano grazie a regole omogenee di interoperabilità transnazionale con il vantaggio di potersi avvalere di documenti elettronici in un formato prestabilito.

Vediamo quali sono le regole stabilite nel nuovo regolamento eIDAS su questa materia.

L'attributo e l'attestato (risultato dell'attestazione) sono definiti nei punti seguenti dell'articolo 3 del regolamento 2024/1183 (eIDAS 2.0):

> *43) "attributo", la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto;*
> *44) "attestato elettronico di attributi", un attestato in forma elettronica che consente l'autenticazione di attributi;*
> *45) "attestato elettronico di attributi qualificato", un attestato elettronico di attributi che è rilasciato da un prestatore di servizi fiduciari qualificato e soddisfa i requisiti di cui all'allegato V;*

Come si vede l'attributo può essere relativo anche ad un oggetto come un sensore elettronico, un apparato meccanico, in generale un'entità che genera dati/informazioni, come accade nel cosiddetto Internet delle cose.

L'attestazione elettronica può essere anche qualificata visto che si tratta di un servizio fiduciario. La definizione specifica l'abbiamo appena proposta.

Nell'ambito operativo è importante anche la fonte autentica definita come di seguito:

> *47) "fonte autentica", un archivio o un sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o di un soggetto privato, che contiene e fornisce gli attributi relativi a una persona fisica o giuridica e che è considerato una fonte primaria di tali informazioni o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa;*

Alla fonte autentica è importante l'associazione con un particolare attestato elettronico, quello rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per su conto. Questo è definito come mostrato di seguito:

> *"46) un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o da un organismo del settore pubblico designato dallo Stato membro per rilasciare tali attestati per conto di organismi del settore pubblico responsabili di fonti autentiche in conformità all'articolo 45 septies e che soddisfa i requisiti di cui all'allegato VII."*

L'appena citato allegato VII è dedicato ai requisiti di questi attestati ed è mostrato di seguito:

ALLEGATO VII
REQUISITI PER GLI ATTESTATI ELETTRONICI DI ATTRIBUTI RILASCIATI DA UN ORGANISMO DEL SETTORE PUBBLICO RESPONSABILE DI UNA FONTE AUTENTICA O PER SUO CONTO

Un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto contiene:

a. *un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che l'attestato è stato rilasciato quale attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto;*
b. *un insieme di dati che rappresenta senza ambiguità l'organismo del settore pubblico che rilascia l'attestato elettronico di attributi e include almeno lo Stato membro in cui tale organismo del settore pubblico è stabilito nonché il suo nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;*
c. *un insieme di dati che rappresenta in modo senza ambiguità il soggetto cui si riferiscono gli attributi attestati; qualora sia usato uno pseudonimo, ciò è chiaramente indicato;*
d. *l'attributo o gli attributi attestati, comprese, ove applicabile, le informazioni necessarie per individuare l'ambito di applicazione di tali attributi;*
e. *l'indicazione dell'inizio e della fine del periodo di validità dell'attestato;*
f. *il codice di identità dell'attestato, che deve essere unico per l'organismo del settore pubblico che rilascia l'attestato, e, se applicabile, l'indicazione del regime per gli attestati di cui fa parte l'attestato di attributi;*
g. *la firma elettronica qualificata o il sigillo elettronico qualificato dell'organismo emittente;*
h. *il luogo in cui il certificato relativo alla firma elettronica qualificata o al sigillo elettronico qualificato di cui alla lettera g) è disponibile gratuitamente;*
i. *le informazioni relative alla validità dell'attestato o l'ubicazione dei servizi a cui è possibile rivolgersi per informarsi in merito.*

Da questo stabilito in questo nuovo regolamento eIDAS 2.0, si comprende che per rilasciare attestati elettronici di attributo è indispensabile disporre di fonti autentiche a maggior ragione se queste sono di natura pubblica.

La normativa operativa sull'attestazione elettronica di attributi è ampia e ad essa è dedicata l'intera sezione 9.

Gli articoli presenti in questa sezione sono sette, dal 45 ter al 45 nonies.

A questi dobbiamo aggiungere gli allegati V, VI e VII (quest'ultimo già mostrato interamente).

Considerando la lunghezza dell'articolato, in questa sede ci concentriamo sul

commento ai principali aspetti dell'attestazione di attributi.

Gli effetti giuridici e l'efficacia probatoria stabiliti nell'articolo 45 ter sono i tradizionali delle norme comunitarie, il formato elettronico è ammesso e la qualifica dell'attributo non è indispensabile in azioni giuridiche.

Gli attributi rilasciati da una fonte autentica del settore pubblico o per suo conto devono avere gli stessi effetti delle attestazioni legalmente rilasciate in formato cartaceo.

Gli attributi così rilasciati sono validi in tutti gli Stati membri.

L'articolo 45 quater è dedicato all'attestazione elettronica di attributi nel settore pubblico. I dati degli attributi non sostituiscono i dati identificativi. Questo è importante nell'uso del Portafoglio Europeo di Identità Digitale.

L'articolo 45 *quinquies* stabilisce le norme per i requisiti per l'attestazione elettronica di attributi. I requisiti sono nell'allegato V e le regole tecniche devono essere coordinate con quelle del Portafoglio Europeo di Identità Digitale.

L'articolo 45 *sexies* tratta della verifica degli attributi rispetto alle fonti autentiche. Sono qui stabilite le tempistiche di rilascio (24 mesi dall'entrata in vigore degli atti di esecuzione) per l'utilizzo da parte dei prestatori di servizi qualificati di attestazione elettronica degli attributi delle fonti autentiche pubbliche. Anche in questo caso gli atti di esecuzione devono essere coordinati rispetto al contesto del Portafoglio e degli attributi elettronici.

L'articolo 45 *septies* stabilisce i requisiti per l'attestazione elettronica di attributi da o per conto di un organismo del settore pubblico responsabile di una fonte autentica.

Questi soggetti dovranno elevate caratteristiche di sicurezza e dovranno possedere adeguate caratteristiche di conformità alle regole comunitarie, in maniera analoga ai soggetti qualificati.

Questo articolo prosegue con le solite regole per l'emissione di regole tecniche e si conclude con l'obbligo per i citati organismi del settore pubblico di fornire un'interfaccia con il Portafoglio Europeo di Identità Digitale, a conferma dello stretto legame tra di esso e gli attributi.

2. Le prospettive operative

Gli attestati elettronici di attributi sono cruciali per il buon funzionamento del Portafoglio Europeo di Identità Digitale. La certificazione degli attributi è (giustamente) considerata fondamentale dal Legislatore comunitario sia per i soggetti pubblici che per quelli privati. Non a caso, la sua messa in opera per i soggetti pubblici che agiscono come fonte autentica è soggetta ad un procedimento di conformità analogo a quello dei prestatori di servizi fiduciari qualificati.

L'elenco pubblico di questi organismi del settore pubblico è analogo a quello dei soggetti che prestano i servizi fiduciari (elenco pubblico di fiducia).

Per concludere questo argomento si ritiene utile per il lettore riportare la parte dell'allegato VI di eIDAS 2.0 che stabilisce l'elenco minimo degli attributi da trattare anche per comprendere, in pratica, di quali informazioni si sta parlando.

Esse sono:
1. Indirizzo
2. Età
3. Genere
4. Stato civile
5. Composizione familiare
6. Nazionalità o cittadinanza
7. Titoli di studio, titoli e patenti
8. Qualifiche, titoli e licenze professionali
8-bis. Poteri e mandati di rappresentanza di persone fisiche o giuridiche
9. Autorizzazioni e licenze pubbliche
10. Per le persone giuridiche, dati finanziari e societari

Queste informazioni, come più volte stabilito nel nuovo regolamento, dovranno essere trattate in conformità con le norme sulla protezione dei dati personali e in coordinamento operativo con le regole del Portafoglio Europeo di Identità Digitale.

3. Conclusioni

In questo articolo abbiamo descritto sinteticamente gli attestati elettronici di attributi e il loro rilascio da parte di soggetti pubblici o privati. Per questi ultimi si tratta di un servizio fiduciario che potrà essere qualificato sulla base delle regole generali già stabilite nel primo eIDAS. Per i soggetti pubblici (denominati nel nuovo regolamento organismi del settore pubblico), specialmente se fonti autentiche, si evince che l'attestazione elettronica di attribuiti è complessa e richiede sforzi operativi per la conformità alla normativa e per il mantenimento della stessa. Il settore pubblico dovrà avere caratteristiche di qualità e sicurezza paragonabili a quelle dei soggetti qualificati.

I soggetti pubblici e privati dovranno agire in modo efficace sulla qualità dei dati in termini di esattezza e disponibilità degli stessi. La protezione dei dati personali è pervasiva all'interno di tutto il nuovo regolamento.

Il Portafoglio Europeo di Identità Digitale, elemento centrale di tutto il sistema, deve interagire in modo efficace con le fonti autentiche e tutte le altri sorgenti di attributi per poter disporre di attestati di attributi affidabili, vista la loro importanza per il funzionamento del sistema dell'identità digitale europea unica e sicura.

La parola chiave da soddisfare per ottenere il successo del sistema cioè l'utilizzo diffuso da parte dei cittadini e delle imprese è fiducia.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 105-125

L'avvento dei QWAC: una svolta epocale nella governance dei certificati SSL

Adriano Santoni

Abstract [IT]: Dopo alcuni anni di discussioni infruttuose, polemiche e accuse reciproche tra le opposte fazioni, il testo finale di revisione del regolamento eIDAS supera l'impasse introducendo l'obbligo di riconoscimento dei Qualified Website Authentication Certificates (QWAC) da parte dei web browser e la visualizzazione "user friendly" delle informazioni in essi contenute. Queste nuove disposizioni, che possono sembrare tecnicalità di secondaria importanza a chi non abbia familiarità con la Web PKI, di fatto segnano un punto di svolta epocale nella governance dei certificati SSL, ma vi sono anche criticità e aspetti poco chiari. Gli attesi benefici nella sicurezza della navigazione sul Web potrebbero essere inferiori alle attese, mentre potrebbero sorgere nuovi problemi.

Abstract [EN]: After a few years of fruitless discussions, controversies and mutual accusations between the opposing factions, the final text of revision of the eIDAS regulation overcomes the impasse by introducing the obligation to recognize Qualified Website Authentication Certificates (QWAC) by web browsers and the "user friendly" display of the information they contain. These new provisions, which may seem like technicalities of secondary importance to those who are not familiar with Web PKI, in fact mark an epochal turning point in the governance of SSL certificates, but there are also critical issues and unclear aspects. The benefits in web browsing security may be less than expected, while new problems may arise.

Parole chiave: eIDAS, PKI, CA, SSL, Certificati SSL, QWAC, Sicurezza sul Web, Phishing.

Sommario: 1. Introduzione – 2. L'autenticazione dei siti web – 3. La governance tradizionale della Web PKI – 4. QWAC: teoria e (poca) pratica – 5. Cosa cambierà con l'eIDAS 2.0 – 6. Aspetti controversi e problematici – 7. Conclusioni.

1. Introduzione

Tra le novità più rilevanti introdotte nella revisione del Regolamento eIDAS, una riguarda ciò che succede "dietro le quinte" quando facciamo una delle cose ormai più frequenti nella vita di tutti i giorni: ci colleghiamo ad un sito web attraverso un normale PC, un tablet o uno smartphone. Nelle primissime fasi di questa operazione, il browser (per es. Chrome, Safari, Edge, Firefox, ecc.) svolge automaticamente una verifica molto importante per la nostra sicurezza: la "autenticazione del sito web". Questa verifica, anche se non risolve tutti i possibili problemi di sicurezza, ci protegge efficacemente da alcuni tipi di attacchi molto pericolosi da parte dei cybercriminali. L'autenticazione dei siti web si appoggia al concetto di "certificato" che è alla base di quasi tutti i servizi fiduciari disciplinati dal Regolamento. I certificati necessari a questo fine sono disponibili da molti anni (da ben prima che fosse emanato il Regolamento), quindi non vi era necessità di una norma europea per risolvere l'esigenza tecnica di base. Senonché i normali certificati usati a questo fine sono sempre stati "governati", nel bene e nel male, da un piccolo numero di aziende nordamericane, il che era considerato un problema dalla CE. Per questa ragione, già nella sua prima edizione del 2014, il Regolamento definisce nell'Articolo 45 un "Certificato qualificato per l'autenticazione dei siti web" (*Qualified Certificate for Website Authentication*, in sigla QWAC) e ne auspica l'utilizzo. Com'è intuibile, questi certificati possono essere emessi solo da Prestatori *Qualificati* di Servizi Fiduciari (QTSP). In pratica, però, fino ad oggi i QWAC sono rimasti pressoché inutilizzati. Questo è dipeso da vari fattori, anzitutto il fatto che i produttori dei browser, in generale, *non considerano affidabili* i QTSP e dunque non accettano i certificati emessi da queste aziende. Inoltre, l'uso dei QWAC non porta alcun vantaggio all'utente rispetto a ciò che si ottiene usando i certificati tradizionali. Nel tentativo di superare lo stallo, la CE ha portato avanti per alcuni anni una discussione con i principali produttori di browser, ma senza costrutto. Alla fine, vista l'impossibilità di un compromesso, la CE ha "tagliato la testa al toro" introducendo nel regolamento 2024/1183 (eIDAS 2.0) l'*obbligo* di riconoscimento dei QWAC da parte dei browser. Queste nuove disposizioni, insieme a molte altre che riguardano temi differenti (per es. lo EUDI wallet), sono riportate nel testo finale[1] di revisione del Regolamento adottato dal Parlamento lo scorso 29 febbraio. In questo articolo, dopo aver descritto le innovazioni introdotte dallo eIDAS 2.0 sul tema dei QWAC e le relative implicazioni, sosterrò che si tratta di cambiamenti che, se pure col tempo potranno portare dei benefici, destano perplessità per varie ragioni. I vantaggi che si otterranno potrebbero essere inferiori alle aspettative, mentre è possibile che emergano nuovi problemi, sia tecnici che di governance. Nel complesso, le nuove misure sembrano rispondere più ad un'esigenza di "sovranità digitale" che non di sicurezza online.

[1] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_EN.pdf

2. L'autenticazione dei siti web

Poiché i QWAC sono rilevanti per l'autenticazione dei siti web, per meglio apprezzare il significato delle novità introdotte dallo eIDAS 2.0 è utile conoscere tale meccanismo. Lo spazio qui disponibile, tuttavia, non consente di soffermarci su questo tema, dunque mi limiterò a richiamarne gli aspetti essenziali per la discussione (chiedo venia ai lettori esperti). Quando lanciamo il browser per collegarci ad un sito web, dopo qualche istante compare la "home page" del sito desiderato e, normalmente, nella barra indirizzo del browser compare anche l'icona di un *lucchetto*[2]. Questa icona indica che il sito è protetto dal protocollo SSL[3], il che garantisce due cose molto importanti: 1) che *il sito web è stato autenticato dal browser*; 2) che *tutti i dati scambiati attraverso Internet* tra il browser e il sito web (come password, numeri di carta di credito, ecc.) *sono crittografati*, rendendo così molto difficile la loro intercettazione da parte di terzi. Ora notiamo il primo punto: che significa dire che un sito web è stato *autenticato*? In questo contesto, significa che il browser ha ottenuto una "prova" affidabile dell'identità del sito, dove con "identità" si intende anzitutto l'indirizzo del sito. Se, per esempio, inseriamo nel browser l'indirizzo "amazon.com" e dopo qualche istante compare l'icona del lucchetto, questo indica che il browser ha ottenuto una prova che il sito web al quale si è connesso è proprio quello che si trova all'indirizzo "amazon.com". Questo può sembrare ovvio, ma non lo è affatto, perché gli hacker sono in grado di "dirottare" le nostre connessioni verso indirizzi *diversi* da quelli che intendevamo raggiungere. Tra l'altro, la crittografia dei dati durante la navigazione subentra solo *dopo* che il sito web è stato autenticato dal browser, pertanto l'autenticazione del sito è necessaria anche per assicurare la *confidenzialità* della navigazione. Ma in che modo il browser ottiene la "prova" che ho citato? Ebbene, la prova si basa su un appropriato *certificato* che il sito web presenta al browser; questo certificato, per essere accettato, *deve contenere l'indirizzo del sito web* e deve essere *emesso da una CA*[4] *che il browser considera affidabile*. E poiché questa verifica si svolge come parte del protocollo SSL, si parla abitualmente di "certificati SSL". L'autenticazione dei siti web è cruciale per proteggerci da alcune gravi forme di truffa online, ma non è *di per sé* sufficiente a contrastare gli attacchi di Phishing. Basti pensare che raramente inseriamo "a mano" nel browser l'indirizzo del sito che vogliamo visitare: più spesso ci limitiamo a cliccare su un link che troviamo su un social network oppure su un banner pubblicitario, e questo può essere già all'origine un link malevolo, cosa di cui è facile non accorgersi (e la nostra disatten-

---

[2] Nel 2023 Google ha tuttavia rimosso il "lucchetto" dal proprio browser ritenendo che sia ignorato dalla maggior parte degli utenti e quindi inutile, se non addirittura dannoso. Ad oggi, gli altri principali browser mostrano ancora il "lucchetto". Per maggiori dettagli si rimanda a https://blog.chromium.org/2023/05/an-update-on-lock-icon.html

[3] https://en.wikipedia.org/wiki/Transport_Layer_Security

[4] Certification Authority, ovvero un prestatore di servizi di certificazione secondo la terminologia eIDAS.

zione, ovviamente, agevola alquanto i cybercriminali). Perciò l'autenticazione dei siti web, seppure molto importante, non è una panacea. Ciò detto, l'aspetto rilevante per il nostro ragionamento è *in che modo il browser verifica l'attendibilità del certificato del sito web*? Qui sta il nocciolo della questione QWAC.

3. La governance tradizionale della Web PKI

Per come hanno funzionato le cose fino ad oggi, un browser considera attendibile il certificato di un sito web solamente se è stato rilasciato da una CA che è *inclusa nell'elenco delle CA attendibili* di quel particolare browser (in tal caso si suole dire che quella CA è "trusted"). Per ottenere questa inclusione, una CA deve farne esplicita richiesta ai browser vendor, dimostrare di operare in piena conformità agli standard del CA/Browser Forum (tra un attimo vedremo di che si tratta) e impegnarsi a rispettare gli *ulteriori requisiti* che ogni particolare browser vendor stabilisce in modo unilaterale. Il CA/Browser Forum[5] (CABF per brevità) è una associazione tra i principali browser vendor e le CA "trusted", e ha lo scopo di sviluppare e pubblicare le regole che tutte le CA "trusted" devono rispettare nella emissione e gestione dei certificati. Si tratta di *centinaia di requisiti*, alcuni dei quali piuttosto gravosi, che hanno la finalità di assicurare che i certificati siano forniti solamente a coloro che ne hanno effettivamente diritto. In particolare, un certificato per un sito web (ossia un "certificato SSL") può essere emesso solo se il richiedente può dimostrare di avere il controllo di quel sito. Questo ovviamente è di cruciale importanza per l'affidabilità di qualsiasi certificato SSL. Ebbene, i browser vendor richiedono alle CA "trusted" di sottoporsi *almeno una volta l'anno* ad una verifica di conformità a tali requisiti, da parte di un auditor qualificato. Questa verifica deve svolgersi nel rispetto di criteri standard, come quelli definiti nella norma europea ETSI EN 319 411. Oltre al rispetto dei requisiti del CABF, una CA che aspira ad essere inclusa nell'elenco delle CA "trusted" di un browser deve anche impegnarsi a rispettare una serie di requisiti *aggiuntivi* che ogni browser vendor stabilisce a propria discrezione nel proprio "Root Program". Si deve notare che il soddisfacimento di queste condizioni non comporta il *diritto* ad entrare nell'elenco delle CA affidabili di quel browser: l'effettiva inclusione è sempre *discrezionale*.[6] [7] Di fatto, però, le richieste di inclusione vengono perlopiù accolte, sebbene dopo un'attesa non breve (talvolta molto lunga). D'altra parte, le CA commerciali che intendono emettere certificati per l'autenticazione dei siti web (più comunemente "certificati SSL"), devono *necessariamente* chiedere ai browser di essere inserite nei relativi elenchi delle CA fidate, perché altrimenti i loro certificati non sarebbero riconosciuti dai browser e

[5] https://cabforum.org/

[6] https://www.chromium.org/Home/chromium-security/root-ca-policy/apply-for-inclusion/

[7] https://www.apple.com/certificateauthority/ca_program.html

dunque sarebbero del tutto inutili (e perciò invendibili). Introduciamo ora un termine conciso per riferirci all'insieme degli attori, delle procedure, delle politiche e delle regole tecniche ed operative che soggiacciono all'autenticazione dei siti web basata sui certificati: questo insieme di elementi interrelati è detto "Web PKI" (Web Public Key Infrastructure). A questo punto dovrebbe essere chiaro al lettore che la Web PKI è governata, ad oggi, da un *piccolo numero di società private statunitensi*: si tratta principalmente di Google, Apple, Microsoft e Mozilla.[8] Viene spontaneo domandarsi se questo stato di cose sia soddisfacente oppure no, specialmente da un punto di vista europeo. Se guardiamo ai dati di fatto, constatiamo che la Web PKI funziona così "da sempre" (almeno negli ultimi 20 anni) e ha sempre assolto in modo efficace ai propri compiti. Non credo si possa onestamente contestare che le regole imposte dai browser vendor alla CA sono *perlopiù* improntate a criteri di sicurezza condivisibili (e di fatto condivisi, nell'ambito del CABF). Inoltre, l'attento e costante monitoraggio che i browser vendor effettuano sull'operato delle CA "trusted" ha permesso, negli anni, di rilevare molte situazioni pericolose per i naviganti; e in quelle occasioni, la capacità dei browser vendor di intervenire *direttamente* con misure anche drastiche (per esempio pubblicando un aggiornamento del browser che disattiva il riconoscimento di una particolare CA) ha consentito il rapido ripristino delle condizioni di sicurezza, seppure con conseguenze talvolta molto severe per la CA responsabile dei problemi[9]. Questa capacità sanzionatoria dei browser, rapida e diretta, è uno "spauracchio" non indifferente dal punto di vista delle CA, mentre dal punto di vista degli utenti (cioè di noi tutti quando visitiamo qualsiasi tipo di sito web) rappresenta ovviamente una forte garanzia di sicurezza. Tuttavia, a volte capita che i browser impongano azioni di rimedio molto onerose da parte di CA che commettono errori veniali. Inoltre, i sanzionamenti applicati dai browser sono *inappellabili*: non esiste un "secondo grado di giudizio" al quale una CA "condannata" possa fare ricorso. C'è poi un altro aspetto che rende la governance della Web PKI da parte dei browser vendor un poco "indigesta", perlomeno dal punto di vista delle CA: alcuni browser vendor fanno *concorrenza* alle CA sul mercato, in quanto essi stessi offrono (gratuitamente) certificati per l'autenticazione dei siti web! Google lo fa attraverso la propria controllata Google Trust Services[10], mentre sia Google che Mozilla sono sponsor e fondatori di Letsencrypt[11]. Analogamente fa Microsoft nell'ambito del proprio servizio "Azure". Pertanto, è comprensibile che per la CE sia sempre stato difficile accettare che nell'ambito della Web PKI il "potere legislativo" e il "potere giudiziario" siano entrambi detenuti da società private nordamericane.

---

[8] Esistono anche web browser prodotti da società europee, per esempio Opera e Vivaldi ma la loro percentuale di utilizzo è molto bassa, e dunque i relativi produttori non hanno, ad oggi, alcuna possibilità di imporre le proprie regole al mercato.

[9] Si pensi al caso Symantec: https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

[10] https://pki.goog/

[11] https://letsencrypt.org/sponsors/

Questo spiega l'introduzione dei QWAC nel Regolamento eIDAS sin dal 2014, e soprattutto la piega che hanno preso le cose a partire dal 2018, quando la CE ha preso coscienza del fatto che i QWAC non stavano "funzionando".

4. QWAC: teoria e (poca) pratica

Esaminiamo ora da vicino i QWAC e il loro ruolo nell'autenticazione dei siti web. Come anticipato, un QWAC non è altro che un tipo di certificato SSL. Ma in cosa si distingue dai più comuni certificati SSL? Questo non si evince dal regolamento eIDAS, ma può essere compreso alla luce delle linee guida pubblicate dall'ENISA[12] nonché delle nome tecniche emanate dall'ETSI. Si vede così che i QWAC sono *tecnicamente* molto simili ai certificati "Extended Validation" che nel 2014 erano già in uso da diversi anni (vedere anche il §6.2). Pertanto, una CA che voglia emettere QWAC non deve fare nulla di diverso da una CA che emette i comuni certificati SSL[13]. Ciò premesso, vi sono però anche notevoli differenze tra i QWAC e i comuni certificati SSL, anzitutto il fatto che un QWAC può essere emesso solo da un QTSP. Chi abbia dimestichezza col Regolamento sa che un TSP, per poter ottenere lo status di *qualificato*, deve superare uno specifico processo che possiamo così riassumere:

1. L'aspirante QTSP si sottopone a una verifica di conformità da parte di un Conformity Assessment Body (CAB) accreditato, ai sensi della norma ETSI EN 319 403-1.
2. Il CAB verifica il rispetto delle norme ETSI EN 319 401, EN 319 411-1 ed EN 319 411-2 da parte del QTSP e rilascia un rapporto di audit (Conformity Assessment Report, CAR) destinato all'organismo di vigilanza (Supervisory Body, SB).
3. Il QTSP sottopone il CAR all'organismo di vigilanza nazionale (SB).
4. Se e quando il SB approva il CAR, il QTSP viene infine inserito nella *Trust List* nazionale[14] in cui viene anche indicato (se del caso) il fatto che questo QTSP è abilitato ad emettere QWAC.

In seguito, la verifica di conformità (audit) a cura del CAB dev'essere ripetuta con frequenza biennale, ma con una visita di "sorveglianza" a distanza di un anno dall'ultimo audit. Qui va notato che gli standard seguiti dal CAB per verificare la compliance dei QTSP sono gli stessi standard ETSI accettati anche dai browser vendor. In particolare, per quanto riguarda i certificati per siti web (come i QWAC), gli

[12] https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-website-authentication-certificates

[13] In verità vi sono minime differenze tecniche, ma sono irrilevanti per questa discussione.

[14] Un file ad accesso libero, pubblicato su Internet a cura del SB, contenente informazioni dettagliate su tutti i QTSP.

standard ETSI EN 319 4xx richiamano i requisiti del CA/B Forum. Pertanto, le regole tecniche a cui devono sottostare i QWAC sono *sostanzialmente* le stesse regole di base che le CA considerate "affidabili" dai browser devono applicare ai normali certificati SSL. Ciò considerato, insieme al fatto che i QTSP sono soggetti al processo di accreditamento che ho descritto e che, in seguito, sono sottoposti a un preciso regime di vigilanza e sanzionamenti, si poteva pensare che i QWAC sarebbero stati usati in modo significativo, dopo l'emanazione dell'eIDAS, come è successo per i certificati di firma digitale, ma così non è stato. Due sono le cause principali del fallimento: anzitutto, i browser vendor, non considerano *affidabile* una CA per il "solo" fatto che è un QTSP. Inoltre, pur essendo possibile ottenere QWAC[15], i browser non li trattano diversamente da qualsiasi altro certificato SSL, pertanto dal punto di vista pratico non fa alcuna differenza se un sito web presenta un QWAC o un altro tipo più comune di certificato. Se poi aggiungiamo il fatto che un QWAC è necessariamente *più costoso* di altri tipi di certificati, è comprensibile che ad oggi di QWAC ne siano stati emessi pochissimi[16], quasi tutti per enti pubblici di paesi nei quali vige l'obbligo di usarli (come per es. in Spagna[17] e in Olanda[18]) oppure per prestatori di servizi di pagamento ai sensi della Direttiva Europea "PSD2".[19] Questa situazione perdura sin dall'entrata in vigore dell'eIDAS, nel 2016. Sin dall'inizio era però abbastanza chiaro che i QWAC non potevano "funzionare" se i browser vendor non li avessero accettati *in quanto tali* e se non li avessero evidenziati all'utente come auspicato dalla CE[20]. I browser però hanno sempre fatto "orecchie da mercante", per cui i QWAC sono rimasti da allora poco più che un'idea, tranne che nei limitati contesti già citati. Sin dal 2018 si sono dunque tenuti diversi incontri tra rappresentanti delle due parti (la CE e i browser vendor), nel tentativo di trovare una soluzione di compromesso, ma questi negoziati sono in definitiva falliti.

5. Cosa cambierà con l'eIDAS 2.0

Nel 2021, vista l'impossibilità di trovare un accordo con i browser vendor sul tema dei QWAC, la CE ha proposto una "***obligation*** *for web-browsers to recognise them and make them more visible*" come parte della più ampia revisione del regolamento eIDAS già in itinere, scatenando un'aspra polemica pubblica. Non mi soffermerò su questa diatriba, ma vorrei menzionare almeno le seguenti prese di posizione:

---

15 Grazie al fatto che alcuni QTSP sono anche delle CA "trusted" nei browser.

16 Meno di 4000 secondo il Censys (https://search.censys.io)

17 https://www.boe.es/buscar/act.php?id=BOE-A-2021-5032

18 https://www.forumstandaardisatie.nl/pdf/739

19 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN

20 Vedere più avanti la discussione sulla "barra verde".

- la "lettera aperta" del novembre 2023, a nome di più di 500 scienziati, esperti di sicurezza e numerose ONG (https://eidas-open-letter.org), nettamente a sfavore dei QWAC;
- la campagna anti-QWAC svolta da Mozilla, attraverso il sito https://security-riskahead.eu/;
- la campagna pro-QWAC svolta dallo ESD[21] (https://www.european-signature-dialog.eu).

Valutando spassionatamente gli argomenti pro e contro, bisogna riconoscere che - sebbene certe accuse fossero esagerate o tendenziose - sono stati evidenziati anche dei problemi non del tutto privi di fondamento (nel capitolo seguente ne prenderò in esame alcuni). Comunque sia, nonostante le critiche, a fine 2023 è stato consolidato il testo finale di revisione del regolamento eIDAS[22] nel quale non solo si impone ma addirittura *si rafforza* ciò che per lungo tempo la CE aveva sperato che i browser accettassero di buon grado. Questo testo è stato infine adottato dal Parlamento Europeo lo scorso 29 febbraio, sfociando così nel c.d. eIDAS 2.0. Vediamo dunque le *principali* novità introdotte dallo eIDAS 2.0 riguardo ai QWAC:

Article 45 - Requirements for qualified certificates for website authentication

> *1. **Qualified certificates for website authentication shall meet the requirements laid down in Annex IV**. Evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.*
> *1a. **Qualified certificates for website authentication** issued in accordance with paragraph 1 **shall be recognised by web-browsers**. **Web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner** […]*
> *1b. **Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1**.*
> *2. **By … [12 months after the date of the entering into force** of this amending Regulation], the Commission shall, by means of **implementing acts, establish a list of reference standards** and when necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. […]*

In sintesi, lo eIDAS 2.0 obbliga i browser ad accettare i QWAC *in quanto tali*, senza necessità che i QTSP emittenti chiedano espressamente ai browser vendor di

[21] Lo ESD si definisce come "a platform of major European electronic signature providers".

[22] https://www.europarl.europa.eu/doceo/document/A-9-2023-0038-AM-006-006_EN.pdf

essere riconosciuti come "trusted". Inoltre, nel collegarsi ad un sito web che presenta un QWAC, i browser dovranno mostrare all'utente in modo "amichevole" le informazioni di identità presenti nel QWAC (ossia il nome dell'organizzazione responsabile del sito web). Queste nuove misure segnano *un punto di svolta radicale* rispetto a come è stata governata la Web PKI fino ad oggi: in pratica, si passerà ad una "governance mista" in cui *sul territorio europeo* si applicheranno anzitutto le regole dettate dalla CE e solo secondariamente e parzialmente quelle dei browser vendor. Non è tutto: viene anche introdotto uno "spazio di manovra" per i browser vendor nell'ambito della gestione degli incidenti di sicurezza:

Article 45a - Cybersecurity precautionary measures

1. ***Web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise Qualified Certificates for Website Authentication and to display the identity data provided in a user-friendly manner***.
2. *By way of derogation from paragraph 1 and* ***only in the event of substantiated concerns related to security breaches or loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates***.
3. ***Where a provider of a web-browser takes precautionary measures*** *pursuant to paragraph 2, the provider of the web-browser* ***shall notify its concerns in writing****, without undue delay, together with a description of the measures taken to mitigate those concerns,* ***to the Commission, the competent supervisory body****, the entity to whom the certificate was issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question.*
4. ***The competent supervisory body shall investigate the issues raised*** *in the notification in accordance with Article 46b(4), point (k).* ***Where the outcome of that investigation does not result in the withdrawal of the qualified status*** *of the certificate,* ***the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end to the precautionary measures*** *referred to in paragraph 2 of this Article.*

In sintesi, qualora un browser adotti delle misure precauzionali a fronte di "violazioni di sicurezza o perdita di integrità di uno o più certificati", dovrà informarne per iscritto anche la CE e l'organismo di vigilanza (SB). Quest'ultimo valuterà le contestazioni avanzate dai browser, e qualora non ritenga opportuno revocare lo status di "qualificato" del QTSP, chiederà al browser vendor di *porre fine* alle suddet-

te misure precauzionali. Anche se questo processo si applica solo ai QWAC, si tratta comunque di *un cambiamento enorme* rispetto alla prassi tradizionale, poiché limita fortemente il potere sanzionatorio dei browser vendor rispetto a quello che possono esercitare fuori dal contesto eIDAS.

6. Aspetti controversi e problematici

Sebbene l'avvento dei QWAC come regolati dallo eIDAS 2.0 possa certamente avere ricadute positive, diversi aspetti della questione QWAC destano perplessità in quanto controversi, problematici, o difficili da interpretare. Di seguito mi soffermo su *alcuni* di questi problemi, senza pretesa di completezza.

6.1 Impatto sulla sicurezza

La ragion d'essere dei QWAC è così enunciata nel Regolamento[23]: "*The issuance of certificates for website authentication is intended to* ***provide users with assurance with a high level of confidence in the identity of the entity standing behind the website****, irrespective of the platform used to display that identity.* ***Those certificates should contribute*** *to the* ***building of trust*** *in conducting business online, as* ***users would have confidence*** *in a website that has been authenticated*". Questo enunciato contiene assunzioni delle quali il legislatore stesso non sembra particolarmente convinto (visto l'uso del condizionale in più punti), ossia che gli utenti si sentiranno più sicuri accedendo a siti web dotati di QWAC, perché ciò comporta un'autenticazione del sito molto affidabile, e che pertanto i QWAC contribuiranno a creare fiducia nello svolgimento del business online. Sembrano assunzioni plausibili, ma esistono varie contro-argomentazioni che non sarebbe onesto ignorare. Vediamo di seguito alcune osservazioni che si possono fare al riguardo.

Un QWAC consente *certamente* un'autenticazione "forte" del sito web *da parte del browser*, ma non più di quanto consentano i normali certificati SSL. Infatti, sulla base delle informazioni contenute nel certificato, il browser può solamente verificare di essersi collegato effettivamente all'indirizzo che gli è stato fornito come input, senza subire dirottamenti. Tuttavia, un QWAC consente all'*utente* di valutare "visivamente" se il sito raggiunto è proprio quello desiderato, grazie al fatto che il QWAC attesta anche l'identità della "*entity standing behind the website*" e che il browser dovrà mostrarla all'utente. Ma anche sotto questo aspetto, non vi sono differenze sostanziali tra i QWAC e i normali certificati SSL "EV", se non che i QWAC verranno presumibilmente meglio evidenziati dai browser nel prossimo futuro. Ciò premesso, è evidente che l'uso dei QWAC potrebbe contribuire al contrasto delle truffe online

[23] Cito dal Considerando 65 dello eIDAS 2.0 in quanto la formulazione era leggermente diversa nello eIDAS 1.0 (2014).

se fosse *obbligatorio*, almeno per alcune tipologie di siti, e (cosa non meno importante) se gli utenti fossero *consapevoli* di un tale obbligo[24]. Senonché l'uso dei QWAC non è affatto obbligatorio: lo eIDAS 2.0 si limita a suggerire timidamente che gli enti pubblici ne facciano uso[25] ma precisa al contempo che l'obbligatorietà non è prevista. Ad oggi, insomma, nulla impone alle aziende "oneste" di dotarsi di un QWAC, per cui non è affatto detto che lo facciano (e si possono immaginare alcune ragioni per volerlo evitare). Può essere che la CE abbia presente questa lacuna e che si riservi di colmarla più avanti, quando i QWAC saranno divenuti di uso comune, ma ad oggi questo non è noto. D'altra parte, anche in assenza di obblighi, è possibile che col tempo i QWAC *prendano piede*, se non altro perché i gestori dei siti apprezzeranno che il browser mostri la loro identità agli utenti (come già avveniva in passato con i certificati "Extended Validation"). Se questo accadrà, gli utenti *impareranno ad aspettarsi* che il browser mostri loro il nome dell'azienda che "sta dietro al sito", quando visitano certe categorie di siti (per es. quelli delle banche), e a quel punto i QWAC aiuteranno effettivamente a contrastare le truffe online. Ma c'è un altro punto di attenzione. Assumendo che un sito web sia dotato di QWAC e che di conseguenza il browser mostri all'utente l'identità del gestore del sito, è ragionevole presumere che l'utente prenda in *attenta* considerazione tali informazioni, prima di decidere se fidarsi o meno di quel sito web? Questo è quantomeno dubbio. Esistono infatti diversi studi[26] [27] [28] [29]che suggeriscono che *il navigante presta scarsa attenzione* agli avvisi mostrati dal browser relativi alla sicurezza della connessione. Non sono studi recenti, e non sono esenti da critiche metodologiche, ma d'altra parte non si conoscono studi alternativi dello stesso tipo (cioè che abbiano analizzato il *comportamento* degli utenti) che supportino la tesi contraria. L'utente è quindi l'anello più debole della catena, il che non è certo una sorpresa. Infine, è facile constatare che quasi tutti i "giganti" del commercio on-line (quali ad esempio Amazon, eBay, Alibaba, Zalando, ecc.) utilizzano sui propri siti dei certificati SSL che non hanno affatto le caratteristiche dei QWAC, e questo non ha certo frenato la crescita dei loro ricavi. Pertanto i QWAC certamente non sono necessari ai fini del "*building of trust in conducting business online*", seppure possano portare benefici. Alla luce delle statistiche sul cybercrime, il problema è piuttosto l'eccessiva fiducia che i naviganti del web ripongono nei siti web che gli viene proposto di visitare.

Riepilogando: l'autenticazione di un sito web in termini di *indirizzo* (dominio) si basa su *automatismi del browser* che sono gli stessi con qualsiasi tipo di certificato SSL. Questo primo livello di autenticazione, importantissimo, non protegge però l'utente dal rischio del Phishing, tanto è vero che la maggioranza dei siti di Phishing

---

[24] La consapevolezza potrebbe essere creata attraverso una campagna informativa.

[25] Considerando 65.

[26] http://www.usablesecurity.org/papers/jackson.pdf

[27] https://ieeexplore.ieee.org/document/4223213

[28] https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-porter-felt.pdf

[29] https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf

sono dotati di un valido certificato SSL[30] [31]. Se però il certificato del sito web attesta anche l'identità del soggetto che "sta dietro al sito", come nel caso dei QWAC (ma non solo), diventa *possibile* un secondo livello di autenticazione - potenzialmente molto utile - che tuttavia dipende in modo cruciale dal *comportamento* dell'utente. E poiché l'uso dei QWAC non è obbligatorio (né si prevede che lo diventi nel prossimo futuro), e gli utenti sono mediamente molto distratti e/o inconsapevoli di tutto ciò, sembra improbabile che l'avvento dei QWAC possa portare un aumento *significativo* della sicurezza online.

6.2 Il ritorno della "barra verde"

Come già visto, lo eIDAS 2.0 si stabilisce che: "***Web-browsers shall ensure*** *that the* ***identity data attested in the certificate*** *and additional attested attributes are* ***displayed in a user-friendly manner***." Pur nella sua vaghezza, il significato del requisito è abbastanza chiaro: il browser deve mostrare all'utente il nome del soggetto titolare del QWAC nonché il suo indirizzo e altri dati di identità se presenti nel certificato. Ad oggi, i browser non mostrano "spontaneamente" queste informazioni, benché sia possibile visualizzarle senza troppe difficoltà. Ma la situazione era ben diversa fino a pochi anni fa, poiché fino al 2018 i web browser, a fronte di un certificato SSL di tipo "Extended Validation" (in sigla EV, molto simile al QWAC), in effetti mostravano all'utente il nome dell'organizzazione titolare del sito, estratto dal certificato. Questa informazione veniva perlopiù evidenziata in colore verde, nella "barra indirizzo" del browser, cosicché si parlava di "barra verde". Introdotta nel 2006, questa funzionalità è stata per lungo tempo considerata normale, tanto è vero che l'uso dei certificati EV era raccomandato in varie norme e regolamenti (per es. nell'ambito bancario/finanziario), ma è stata rimossa dai browser tra il 2018 e il 2019 perché i produttori stessi la consideravano inutile[32]. Tuttavia, è evidente che la CE si è ispirata, nel concepire i QWAC, ai certificati EV, come confermato da varie fonti[33], non prevedendo che pochi anni dopo i browser avrebbero rimosso la "barra verde". Ora però lo eIDAS 2.0 impone ai produttori dei browser la re-introduzione di una funzionalità che essi stessi hanno poco tempo fa rimosso. Come reagiranno a questa imposizione? È purtroppo probabile che i browser si comporteranno in modo differente l'uno dall'altro (come già avveniva in passato con i certificati EV), a meno che non si imponga loro il rispetto di uno standard (che però, ad oggi, non è stato ancora definito e non è chiaro se sia previsto). Assisteremo al ritorno della "barra verde", magari con un diverso colore, e vedremo comparire l'EU Trust Mark? Lo capiremo meglio nei prossimi mesi. Peraltro, sui dispositivi mobili (quali smartphone

[30] https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

[31] https://www.phishlabs.com/blog/more-than-half-of-phishing-sites-use-https

[32] https://duo.com/decipher/chrome-and-firefox-removing-ev-certificate-indicators

[33] Si vedano ad esempio le linee guida pubblicate dall'ENISA sul tema dei QWAC.

e tablet) può essere difficile soddisfare il requisito a causa della ridotta dimensione dello schermo[34], ma nondimeno lo eIDAS 2.0 ne chiede il supporto ("*irrespective of the platform used to display it*"). Questo non è certo un problema secondario, visto che gli utenti "mobili" sono molto più esposti al phishing degli utenti "desktop".

6.3 La consultazione delle Trust List

La fase iniziale del colloquio tra il browser ed un sito web, in cui il browser verifica il certificato del sito, deve concludersi nel più breve tempo possibile, possibilmente in una frazione di secondo, affinché la c.d. "user experience" si mantenga soddisfacente. Gli utenti tendono infatti a spazientirsi, se il sito richiamato non compare al più presto, perciò i produttori dei browser e gli ingegneri che sviluppano protocolli sicuri di comunicazione investono molto lavoro per fare in modo che questa fase "non produttiva" si concluda con la massima rapidità. Ciò premesso, lo eIDAS 2.0 impone di fatto ai browser di *consultare le Trust List* quando l'utente si collega ad un sito che presenta un QWAC, per verificare che il QWAC sia emesso da un QTSP abilitato. Considerando però che le Trust List sono ad oggi una trentina, che sono soggette ad aggiornamenti abbastanza frequenti, e che alcune sono relativamente "pesanti", questa consultazione potrebbe comportare dei problemi anzitutto prestazionali, secondo come verrà realizzata, almeno su alcune piattaforme (es. smartphone). Se poi questa consultazione fosse attuata attraverso un servizio esterno (per esempio quello gestito dalla stessa Commissione[35]), ne deriverebbero dei problemi di *privacy*, perché questo servizio esterno inevitabilmente riceverebbe dai browser informazioni che consentirebbero di risalire ai siti che determinati utenti hanno visitato. Anche se questo tracciamento fosse solo potenziale, probabilmente non sarebbe accettabile. Queste difficoltà sono senz'altro superabili, in qualche modo, ma non sono trascurabili e potrebbero introdurre dei ritardi nel "dispiegamento" dei QWAC. Alla fine, in informatica quasi tutto è possibile, ma talvolta al prezzo di compromessi o di eccessive complicazioni che aumentano il rischio dei "bugs" e dunque di vulnerabilità di sicurezza.

6.4 Applicabilità ai Web Services

Sembra che il legislatore abbia ignorato il fatto che il Web viene usato massicciamente anche in modo *non interattivo*, ossia attraverso una comunicazione *automatica* tra un sistema "server" (tecnicamente simile ad un sito web) che eroga determinati servizi e un sistema "client" (assimilabile al browser) che ne fruisce senza bisogno di presenza umana. Questa tecnica ("Web Services") è in uso da molti anni ed è a dir poco essenziale per il business online che il Regolamento intende

[34] https://www.cise.ufl.edu/~traynor/papers/amrutkar-isc12.pdf

[35] https://eidas.ec.europa.eu/efda/swagger-ui/index.html

agevolare. In tutti i più importanti settori economici si fa un uso amplissimo di Web Services: e-commerce, servizi bancario-finanziari, telco, sanità, trasporti e logistica, ecc. Anche queste comunicazioni richiedono l'autenticazione del server attraverso un certificato SSL, senonché sul lato client non si usano i normali web browser bensì dei prodotti software che svolgono la stessa funzione operando in modo automatico. Pertanto, il requisito che "*the identity data attested in the certificate and additional attested attributes are* ***displayed*** *in a user-friendly manner*" (Art. 45, comma 1, dello eIDAS 2.0) evidentemente in questi casi non ha senso. Più serio sembra il problema di come possano questi software validare un QWAC – nel caso in cui il server presenti un tale certificato – senza scendere a compromessi in termini di prestazioni e di sicurezza[36]. Dato che lo eIDAS 2.0 non fa alcun cenno a questo caso, è difficile capire se i server che erogano Web Services potranno utilizzare QWAC oppure no, ma in entrambi i casi lo scenario sembra problematico.

6.5 Due pesi e due misure?

Al comma 1b del nuovo Articolo 45, troviamo quella che (apparentemente) è la novità più sorprendente: "***Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1***." Questa è una disposizione decisamente controintuitiva, perché di solito in un Regolamento si stabiliscono requisiti *minimi*, non requisiti massimi. Proviamo a capire meglio cosa può significare questo passaggio. Nel comma 1 si stabilisce unicamente che i QWAC "*shall meet the requirements laid down in Annex IV*" e nell'Allegato IV si trovano solo requisiti di alto livello sul contenuto del certificato. Nel comma 2, infine, si stabilisce che entro 12 mesi sarà pubblicato un elenco di standard tecnici da applicarsi ai QWAC ai fini delle verifiche di conformità. Sembra quindi che non si potranno imporre ai QWAC altri requisiti che quelli stabiliti nell'Allegato IV e negli standard tecnici che più avanti la CE indicherà. *Se questa fosse la corretta interpretazione* del comma 2b, le conseguenze sarebbero sconcertanti. Consideriamo infatti che nella "normale" Web PKI, come l'abbiamo conosciuta fino ad oggi, affinché una CA sia considerata affidabile dai browser, è necessario che tale CA si impegni a rispettare non solamente gli standard emanati dal CABF, come è richiesto anche ai TSP che emettono QWAC, ma anche e anzitutto il "Root Program" di quel particolare browser [37] [38] [39], il che significa dover rispettare *un insieme più ampio di requisiti*. Ma non è tutto: i browser vendor, infatti, impongono alle CA "trusted" *anche ulteriori requisiti* che, seppure non inclusi nei loro "Root Program", di

[36] Qui naturalmente ci riferiamo solo ai QWAC emessi da CA che non sono incluse negli elenchi delle "CA affidabili" di tali software; tali elenchi coincidono, di fatto, con gli elenchi usati dai web browser interattivi.

[37] https://www.chromium.org/Home/chromium-security/root-ca-policy/

[38] https://www.apple.com/certificateauthority/ca_program.html

[39] https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/

fatto sono obbligatori. Per fare un esempio di particolare rilevanza, sia Google che Apple richiedono che tutti i certificati SSL emessi dalla CA siano sottoposti al processo di "Certificate Transparency".[40] Ebbene, secondo l'interpretazione del comma 1b che qui stiamo ipotizzando, i QTSP sarebbero *esentati* dal requisito della Certificate Transparency, nonché da una serie di altri impegnativi requisiti dei browser vendor. Ne conseguirebbe una Web PKI dove si applicano "due pesi e due misure", il che certo non gioverebbe alla sicurezza né alla governabilità (oltre a essere palesemente ingiusto). Questo sembra strano e difficile da credere, quindi potrebbe trattarsi di un'errata interpretazione del comma 1b. In effetti, nel Considerando 65 si trova un passaggio che pare contraddire quanto previsto dal comma 1b: "*The obligation of recognition and interoperability of and support for qualified certificates for website authentication* ***does not affect the freedom of providers of web-browsers*** *to ensure web security,* ***domain authentication*** *and the encryption of web traffic* ***in a manner and by means of technology that they consider to be the most appropriate***." Tuttavia, i Considerando (Recitals) *non sono prescrittivi* e dunque non possono modificare quanto stabilito nel "corpo" vero e proprio del Regolamento. Peraltro, anche l'Articolo 45a (*Cybersecurity precautionary measures*) introdotto nello eIDAS 2.0, già discusso nel capitolo 5, configura una disparità di trattamento tra le CA che sono "trusted" nei browser e quelle che invece i browser dovranno considerare affidabili *obtorto collo* (ovvero i QTSP), poiché solo i QTSP potranno godere di un "secondo grado di giudizio". Questo problema (la coesistenza di due schemi di sicurezza per il Web basati su regole differenti) potrebbe mitigarsi solo se i browser vendor trasferissero al CABF la responsabilità di stabilire *tutti* i requisiti che essi ritengono indispensabili (giacché le norme ETSI EN 319-4xx richiamano i regolamenti del CABF), oppure se chiedessero all'ETSI di incorporare tali requisiti nelle norme EN 319-4xx. Per esempio, i browser vendor potrebbero proporre il recepimento della "Certificate Transparency" nelle norme ETSI 319-4xx oppure negli standard del CABF.

6.6 Cosa può dirci un QWAC

La possibilità per l'utente di vedere il nome della società che "sta dietro" ad un sito web è certamente utile, e può contribuire ad aumentare la sicurezza online, ma solo fino a un certo punto. Bisogna infatti considerare che i nomi delle aziende non sono univoci a livello globale né a livello nazionale: esistono le omonimie. Se il browser mi informa che il sito web che sto visitando è gestito dalla società "ABCD" (nome di fantasia), potrebbe non trattarsi della stessa "ABCD" che avevo in mente. Nulla vieta, infatti, che esistano diverse aziende denominate "ABCD": di norma è tollerata la registrazione di ditte o marchi anche uguali che però operino in settori diversi. Certo, se il browser mi mostra anche l'indirizzo dell'azienda (come si suppo-

[40] https://certificate.transparency.dev/

ne che avverrà, ai sensi del nuovo Art. 45) l'ambiguità si riduce, ma l'informazione mi sarà utile solo se vi presto attenzione e se ho il tempo, la voglia e la capacità di verificarla in caso di dubbi. Per esempio, se il browser mi informasse che il sito a cui mi sono collegato è gestito da una "Amazon, Inc." con sede a Bakersfield (CA), mi accorgerei che non si tratta della "vera" Amazon che ha sede a Seattle (WA)? Probabilmente no. Molto dipende dalle mie precedenti conoscenze e conseguenti aspettative, dalla mia attenzione, e da altri fattori concomitanti. Potrebbe anche trattarsi di un'azienda che ha un nome *graficamente* molto simile a quello che mi attendevo (per esempio "A8CD S.p.A."), al punto da non accorgermi della differenza. Guardando le cose da una differente prospettiva, è molto improbabile che gli hacker utilizzeranno certificati QWAC, a maggior ragione che cerchino di farsi passare per aziende molto note e con marchi registrati in tutto il mondo. L'uso di tali certificati, infatti, agevolerebbe le indagini delle forze di polizia volte a individuare gli autori dei cyber-crimini. Del resto, ad oggi le statistiche sul cybercrime non segnalano casi significativi in cui certificati "Extended Validation" (pressoché identici ai QWAC) siano stati usati su siti malevoli. Pertanto, il fatto stesso che il browser mi mostri informazioni sull'azienda che "sta dietro" al sito, anche se poi non presto molta attenzione a queste informazioni, sarà generalmente un *buon segno*; ma quanto sia rilevante ai fini della sicurezza è opinabile, e comunque dipende da vari altri fattori (vedere anche il §6.1).

6.7 Le ricadute economiche

Alcuni oppositori dei QWAC hanno sostenuto che il vero motivo dietro alle nuove misure normative è l'avidità delle CA commerciali la quali, in parole povere, sperano di arricchirsi indebitamente vendendo certificati inutili a caro prezzo. Vediamo di capire meglio. Il fatto che un certificato QWAC debba avere un prezzo relativamente elevato, rispetto ai certificati di tipo più comune (ottenibili anche gratuitamente), è evidentemente più che giustificato. Le verifiche che una CA (TSP) deve svolgere, prima di emetterli, hanno un costo che deve essere remunerato. Ma anche considerando questo fatto ovvio, è plausibile sostenere che le CA otterranno grandi ricavi dalla vendita dei QWAC? Per valutare la sensatezza di questa accusa, possiamo esaminare l'incidenza dei normali certificati "Extended Validation" (assimilabili ai QWAC) sul totale dei certificati per siti web che sono stati mai emessi. Le cifre che fornirò, ottenute dalla consultazione del Censys, sono da prendere con prudenza[41], tuttavia risulta chiaramente che i certificati "a pagamento" sono una percentuale minima di tutti i certificati mai emessi, e tra questi i certificati EV sono addirittura meno dell'1%. Se poi consideriamo che le CA che offrono EV sono numerose[42], che dunque la concorrenza è elevata, e che di conseguenza i prezzi sono in continuo calo,

[41] L'autore dell'articolo resta a disposizione dei lettori interessati a conoscere la procedura usata per ottenere queste cifre.

[42] E numerosi sono anche i QTSP pronti ad emettere QWAC, come risulta dalle Trust List europee.

si comprende che l'incidenza degli EV sui ricavi delle CA è molto bassa. Pertanto, anche se è possibile che le nuove norme portino ad un significativo aumento della domanda di QWAC, non sembra verosimile che questo incremento possa tradursi in grandi ricavi per le CA.

6.8 Sorveglianza dei cittadini?

Premetto che *non ritengo questo un tema importante* nell'ambito di una valutazione generale dei QWAC, ma penso sia utile fornire al lettore alcune delucidazioni. Come già accennato, il principale argomento usato dai browser vendor e da altri oppositori dei QWAC è stato quello della presunta volontà della CE di agevolare la "sorveglianza" dei cittadini. Costoro sostengono che le nuove disposizioni consentono ai paesi membri UE di inserire *surrettiziamente* una CA nella propria Trust List, favorendo così l'*intercettazione* del traffico web ("Man-In-The-Middle"), a *discapito della privacy dei cittadini*. Mozilla, in particolare, ha denunciato questo pericolo attraverso una campagna di informazione dai toni molto allarmanti:[43] Ma come funzionerebbe questa sorveglianza, in pratica? Come abbiamo già visto, il fatto che una CA sia presente in una Trust List e abilitata all'emissione di QWAC consentirà tecnicamente a quella CA di emettere certificati che i browser saranno *obbligati* ad accettare. Ma poiché il browser non può "sapere" se i certificati che incontra sono stati *realmente* emessi nel rispetto delle regole, *in teoria* una CA potrebbe rilasciare dei QWAC a soggetti che non ne hanno diritto (per esempio organi di polizia, servizi segreti, ecc.) in quanto non proprietari del sito indicato nel QWAC. In pratica, una CA "malandrina" potrebbe rilasciare un QWAC per il sito "amazon.com" ad un soggetto che non ha nulla a che fare con la ben nota società Amazon. E poiché l'utente medio non sarebbe minimamente in grado di accorgersi del problema, quel soggetto potrebbe - attraverso particolari tecniche - intercettare le comunicazioni degli utenti con il vero sito di Amazon, riuscendo così a tracciare i loro acquisti e infrangendo la loro privacy. Sembra uno scenario impossibile, alla luce delle tante regole che le CA devono rispettare. Per definizione, una CA è una "terza parte fidata": come può essere che tradisca in modo così enorme la propria missione? Eppure, nel 2013 l'agenzia governativa francese ANSSI, che a quel tempo era anche una CA "trusted" nei browser, ha rilasciato certificati "fasulli" che consentivano l'intercettazione del traffico web.[44] Quello dell'ANSSI è l'unico caso *europeo* di cui si abbia notizia, ma casi analoghi si sono verificati anche in altri paesi quali Turchia, Kazakistan, Russia e Cina.[45] Quindi stiamo parlando di cose che a volte *capitano*. Ora, va detto che talvolta possono esserci delle valide ragioni per intercettare le comunicazioni di *alcuni* cittadini, per esempio il contrasto alla criminalità organizzata e al terrorismo, ma è

[43] https://last-chance-for-eidas.org/

[44] Anche qui, mi si perdoni la semplificazione del resoconto, per non appesantire la lettura.

[45] https://last-chance-for-eidas.org/art45interception.html

verosimile che venga fatto in questo modo? Sembra piuttosto improbabile, perlomeno in Europa, anche perché il Regolamento non lo prevede[46]. In teoria, i paesi membri UE non possono inserire "a piacere" una nuova CA (QTSP) nella propria Trust List. Il processo previsto dal Regolamento, infatti, impone una precisa serie di passaggi a carico di diversi soggetti, come abbiamo già ricordato nel cap. 4. Si tratta di un processo non facilmente aggirabile, se tutti gli attori rispettano le regole. Ma a volte capita (per fortuna raramente) che le regole vengano infrante, talvolta addirittura da coloro che hanno il compito di farle rispettare.[47] La conclusione che traiamo da queste considerazioni è che, sebbene l'accusa rivolta alla CE sia eccessivamente allarmistica e male argomentata, il rischio denunciato non è del tutto inverosimile, per quanto improbabile. Sembra però un argomento molto debole per opporsi ai QWAC.

6.9 Vigilanza e sanzioni

Per farsi un quadro più completo delle ragioni *pro* e *contro* i QWAC, è importante considerare anche le differenze tra i due schemi di governance (quello della Web PKI tradizionale e quello previsto dal Regolamento) per quanto riguarda *la vigilanza e il sanzionamento* delle CA che infrangono le norme. Infatti anche le CA commettono errori, e certi tipi di errori possono mettere a rischio la sicurezza di *molti* utenti (tutti coloro che accedono ad un sito web) e dunque sono potenzialmente molto gravi. Dunque è importante, per la sicurezza di tutti, che ci sia una scrupolosa vigilanza sull'operato delle CA e che, nei casi più gravi, ci siano sanzionamenti commisurati alla gravità dei problemi causati. Per quanto riguarda la governance tradizionale della Web PKI, abbiamo già visto che gli stessi browser vendor attuano un monitoraggio assiduo dell'operato delle CA e sono in grado di "comminare" vari tipi di sanzionamenti, non pecuniari ma comunque efficaci e talvolta molto pesanti, che di fatto sono stati applicati molte volte nel corso del tempo[48]. Questi sanzionamenti "tecnici" sono di fatto *inappellabili*, perché non sono regolati da norme di legge, e dopo tutto il proprietario di un software può fare quello che crede meglio col proprio prodotto. Va anche detto che, riguardo agli incidenti che hanno coinvolto le CA "trusted", è disponibile al pubblico un'ampia documentazione - come forse è giusto che sia quando è in gioco la sicurezza di tutti - quindi è agevole valutare se i sanzionamenti applicati dai browser vendor siano stati o meno commisurati alla gravità dei problemi rilevati. Nel quadro del Regolamento le cose funzionano diversamente. Il Supervisory Body (SB) è il soggetto incaricato di supervisionare l'operato dei TSP e di applicare sanzioni nel caso di trasgressioni al Regolamento. Nel caso dei QTSP, tra l'altro, l'attività di supervisione deve svolgersi "*ex ante*" ed "*ex post*".

---

[46] Ma le norme nazionali di qualche paese potrebbero consentirlo in circostanze particolari.

[47] Si noti che l'ANSSI è il Supervisory Body francese ai sensi del Regolamento!

[48] https://www.researchgate.net/publication/334789185_A_Complete_Study_of_PKI_PKI%27s_Known_Incidents

In altre parole, il SB deve svolgere ispezioni *anche in modo preventivo*, e non solo quando un incidente si è ormai verificato. E laddove rilevi delle trasgressioni, il SB deve imporre al TSP di rimediare. Nel Regolamento si stabilisce inoltre che, quando le azioni correttive richieste ad un QTSP non sono attuate nei tempi concessi, il SB può anche (nei casi più gravi) revocare lo status "qualificato" di quel QTSP, in toto o limitatamente ad alcuni dei suoi servizi, aggiornando conseguentemente la Trust List. Questo schema non è solo teorico: gli organismi di vigilanza dei vari paesi membri UE effettivamente svolgono ispezioni periodiche presso i QTSP, rilevano problemi, ed applicano sanzioni. È però difficile stabilire se la "sanzione massima" (la revoca dello status di *qualificato* di un QTSP o di qualche suo servizio) sia mai stata applicata per cause del tipo qui discusso, tantomeno conoscere le esatte motivazioni, perché gli SB non sono tenuti a pubblicare informazioni al riguardo, e di conseguenza è difficile valutare se siano più o meno "severi" dei browser vendor nel giudicare situazioni di comparabile gravità, specie nel caso dei servizi di emissione di QWAC che, come già evidenziato, fino ad oggi sono stati erogati in misura trascurabile. Possiamo comunque immaginare che i SB dei vari paesi membri UE non siano tutti uguali in termini di risorse, competenze, orientamento, pertanto la loro efficacia nell'individuare, valutare, e sanzionare le trasgressioni dei QTSP potrebbe facilmente variare da un paese all'altro.[49]

Con l'entrata in vigore dello eIDAS 2.0, la logica generale che ho descritto non cambia in modo sostanziale: viene confermato il ruolo-cardine del SB, il suo compito di vigilanza e il suo potere-dovere di sanzionamento dei QTSP che non rispettano le regole. Ci sono però le nuove disposizioni che, nel caso dei QWAC, riconoscono un ruolo ai browser vendor nel processo di gestione degli incidenti di sicurezza, come abbiamo già visto nel capitolo 5. Tutto ciò considerato, non è agevole valutare se lo schema di vigilanza e sanzionamenti stabilito dal Regolamento, in particolare per quanto si applica ai QWAC, sia "migliore" di quello tradizionalmente vigente nella Web PKI. Alla luce di quanto sappiamo ad oggi, lo schema eIDAS sembra tutelare maggiormente le CA dal rischio di sanzionamenti molto severi, mentre non è chiaro quanto sarà vantaggioso per la sicurezza degli utenti.

6.10 Un diverso regime di responsabilità

Un argomento che è stato spesso utilizzato dai fautori dei QWAC è quello del "regime di responsabilità" al quale sono soggetti i QTSP. Certamente si tratta di un regime ben diverso da quello che ha finora caratterizzato la Web PKI. Infatti l'eIDAS stabilisce che un QTSP deve risarcire i danni eventualmente causati a terzi, a meno che non dimostri di aver agito senza intenzione o negligenza. Oltre a questo, come abbiamo già visto, è previsto un potenziale sanzionamento da parte del

[49] È noto almeno un caso in cui un QTSP è stato rimosso dall'elenco delle CA affidabili dei browser, a causa di una lunga serie di incidenti, ma il SB apparentemente non ha ritenuto che fosse il caso di revocare lo status di "qualificato" di quel QTSP.

SB. Tra l'altro, lo eIDAS 2.0 precisa che "***Any natural or legal person who has suffered material or non-material damage*** *as result of an infringement of this Regulation by trust service providers* ***shall have the right to seek compensation*** *in accordance with Union and national law*". A questo proposito bisogna notare che, poiché un QWAC autentica non una persona fisica bensì di un sito web, l'emissione "errata" di un QWAC (che avvenga per dolo o per semplice negligenza) può avere conseguenze *molto più gravi* di quelle che possono derivare da un errato certificato di firma digitale, in quanto impattano su una *molteplicità di utenti* (tutti quelli che visitano il sito per cui è stato emesso il QWAC). Pertanto, i rischi che un QTSP corre nell'erogazione dei QWAC sono maggiori di quelli che corre nel contesto di altri servizi di certificazione. Tuttavia, nell'ambito della governance tradizionale della Web PKI, le CA "trusted" non hanno alcun obbligo di risarcire coloro che eventualmente subiscono danni per dolo o negligenza della CA[50], pertanto ogni CA si regola come ritiene opportuno. È dunque corretto affermare che i QWAC sono soggetti a un regime di responsabilità ben diverso da quello che vige per i "normali" certificati SSL. Se poi, in pratica, questa diversità sia rilevante per la diffusione dei QWAC e (cosa più importante) per la sicurezza online, lo capiremo solo in futuro.

7. Conclusioni

Fino ad oggi, le regole che governano la Web PKI sono state dettate da poche società private basate negli USA: si tratta delle "Big Tech" come Google, Apple, Microsoft e poche altre, produttrici tra l'altro dei web browser più diffusi nel mondo. Queste società decidono in piena autonomia quali Certification Authority (TSP in terminologia eIDAS) sono riconosciute dai propri browser, e dunque quali CA possono emettere i *certificati* che sono necessari per *l'autenticazione dei siti web*: un meccanismo molto importante ai fini della sicurezza della navigazione. L'inclusione di una CA nell'elenco delle CA fidate ("trusted") di un browser è soggetta al soddisfacimento di numerosi requisiti tecnico-operativi standardizzati dal CABF, ma anche di ulteriori requisiti stabiliti da ciascun browser vendor. La vigilanza sull'operato delle CA è svolta dagli stessi browser vendor i quali, a fronte di incidenti di sicurezza o di gravi non-conformità, possono applicare sanzionamenti anche molto severi alle CA incriminate, fino al loro completo disconoscimento ("distrust"). Tali sanzionamenti sono peraltro inappellabili. Questo schema di governance, in atto da molti anni, ha garantito sinora un elevato livello di sicurezza e di interoperabilità. Tuttavia, i browser vendor hanno talvolta assunto decisioni opinabili in modo unilaterale, a cui le CA "trusted" hanno dovuto giocoforza adeguarsi. Con l'avvento dell'eIDAS 2.0, la situazione cambierà radicalmente: i paesi membri UE potranno decidere in piena

[50] Fanno eccezione i browser vendor che, invece, devono essere risarciti della CA che causano danni, come stabilito dai regolamenti del CABF.

autonomia che determinate CA qualificate (QTSP) possono emettere certificati SSL di tipo QWAC che i browser vendor *dovranno* riconoscere a priori come affidabili e *dovranno* evidenziare all'utente. I browser vendor si sono fortemente opposti all'introduzione di questi obblighi, adducendo argomenti in parte validi, in parte assai discutibili, ma anche le tesi a favore dei QWAC presentano lacune e debolezze. Alla fine, tuttavia, lo eIDAS 2.0 risolve l'impasse in modo draconiano, confermando l'obiettivo iniziale del legislatore. Assisteremo dunque a cambiamenti molto rilevanti nella governance della Web PKI, ma le implicazioni non sono del tutto chiare, e i benefici che si otterranno potrebbero essere inferiori alle attese. Se, da un lato, sarà certamente utile per il navigante avere visibilità del soggetto che "sta dietro" ad un sito web, dall'altro non è scontato che questo comporti una riduzione *significativa* delle truffe online, tantomeno che possa incrementare il business digitale, mentre è possibile che le nuove disposizioni facciano sorgere nuovi problemi di non semplice soluzione.

Bibliografia

- 2021/0136 (COD): Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. 6 December 2023.
- ENISA. *Security guidelines on the appropriate use of qualified website authentication certificates*. Version 2.0 Final. December 2016.
- Nicolas Serrano, Hilda Hadan, and L. Jean Camp. *A Complete Study of P.K.I. (PKI's Known Incidents)*. In The 47th Research Conference on Communications, Information, and Internet Policy, 2019. TPRC.
- Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. *The Emperor's New Security Indicators*. In IEEE Symposium on Security and Privacy (S&P'07).
- Jackson, Collin; Daniel R. Simon; Desney S. Tan; Adam Barth. "*An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks*". Usable Security 2007.
- Felt A. P., Reeder R. W., Ainslie A., Harris H., Walker M., Thompson C., Acer M. E., Morant E., and Consolvo S., 2016. "*Rethinking connection security indicators*". In Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS'16).
- Devdatta Akhawe and Adrienne Porter Felt. "*Alice in warningland: A large-scale field study of browser security warning effectiveness*". In Proceedings of the USENIX Security Symposium, 2013
- Rana Alabdan. "*Phishing Attacks Survey: Types, Vectors, and Technical Approaches*". Future Internet 2020.
- Chaitrali Amrutkar, Patrick Traynor, Paul C. Oorschot. *Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?* Information Security, 2012, Volume 7483.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 126-144

Dalla conservazione digitale all'e-archiving. I requisiti che un qualified trust service provider deve posedere per erogare il servizio di e-archiving: prospettive e scenari per il mercato

Patrizia Sormani

Abstract [IT]: I servizi fiduciari sono al centro del Regolamento europeo 2024/1183 e per essere erogatore degli stessi sono richieste importati garanzie al prestatore di servizi.

Il Regolamento eIDAS contiene molte novità di rilievo, tra cui una – l'evoluzione dell'e- archiving, che potrebbe avere un impatto rilevante sul mercato italiano ed europeo. Si esamina il passaggio cruciale dalla conservazione digitale come intesa in Italia all'e-archiving, mettendo in luce i requisiti essenziali che un fornitore di servizi fiduciari qualificati e non deve possedere. È rilevante esaminare poi gli impatti di tutto ciò su un mercato in evoluzione. Diversi sono i cambiamenti previsti ed è importante focalizzarsi sui requisiti richiesti per comprendere anche l'impatto sul mercato e su un Know How unico in Italia. Allo stato attuale è fondamentale trovare un'armonizzazione tra la norma europea e la norma italiana, per comprendere le sfide e le opportunità nel contesto dell'e-archiving e per anticipare le tendenze che plasmeranno il futuro di questo settore cruciale.

Abstract [EN]: Fiduciary services are at the heart of the European Regulation and important guarantees are required from the service provider to provide them.

The 2024/1183 Regulation contain many important novelties, including one - the evolution of electronic archiving - that could have a significant impact on the Italian and European market. The crucial transition from digital preservation as understood in Italy to electronic archiving is examined, highlighting the essential requirements that a qualified and non-qualified trust service provider must possess.

It is then important to examine the impact of all this on an evolving market. Several changes are expected, and it is important to focus on the requirements in order to also understand the impact on the market and on a unique know-how in Italy. Currently, it is crucial to find harmonisation between the European and Italian standards, to understand the challenges and opportunities in the context of electronic archiving, and to anticipate the trends that will shape the future of this crucial sector.

Parole chiave: fiducia nelle transazioni elettroniche, Regolamento europeo 2024/1183, conservazione digitale, e-archiving, requisiti, normativa.

Sommario: 1. Introduzione al tema - 2. Il panorama dei servizi fiduciari qualificati e non alla luce del nuovo Regolamento 2024/1183 - 3. Dalla conservazione all'e-archiving - 4. I requisiti che un fornitore di servizi fiduciari di e-archiving deve possedere - 5. Gli impatti su un mercato in evoluzione alla ricerca di un'armonizzazione tra normativa italiana e normativa europea - 6. Conclusioni verso il futuro che ci attende

1. Introduzione al tema

Il Regolamento eIDAS vigente, Regolamento (UE) n. 910/2014 in vigore dal 1° luglio 2016 meglio definito come Regolamento europeo su electronic Identification Authentication and Signature è stato aggiornato con il nuovo regolamento 2024/1183.

Il Regolamento eIDAS vigente, ha avuto come scopo, al momento della sua emanazione, la volontà di mirare a rafforzare la fiducia nelle transazioni elettroniche e nel mercato interno all'Unione, allo scopo di fornire una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche. Esso definisce infatti servizi fiduciari digitali quei servizi elettronici che si occupano della creazione, verifica e convalida di molte autenticazioni informatiche esistenti. Un servizio elettronico è definito servizio fiduciario quando è in grado di essere trust, cioè, creare tra le parti di una transazione elettronica la fiducia necessaria per fare assoluto e legittimo affidamento nella transazione stessa, nei suoi interlocutori e nell'obbiettivo che la stessa si prefigge di raggiungere.

Nello specifico si stratta di servizi di creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato; certificati relativi a tali servizi; servizi di creazione, verifica

e convalida dei certificati di autenticazione di siti web; servizi di conservazione di firme; sigilli o certificati elettronici relativi a tali servizi.

Per contro viene poi definito servizio fiduciario qualificato un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.

È importante quindi fin da subito elaborare e memorizzare il tema che posso avere due livelli di servizi fiduciari previsti dal Regolamento: qualificati o meno e certamente questo impatterà sugli effetti giuridici degli stessi. Come recita lo stesso Regolamento si tratta perlopiù di servizi informatici offerti dal mercato, generalmente a pagamento. Di fatto vedremo come un servizio fiduciario richieda una serie di requisiti affinché possa essere prestato nel rispetto della normativa; il rispetto di questi requisiti richiede che vengano sopportati oneri a vario titolo da parte di chi presta tali servizi, e pertanto è pressoché ovvio che lo stesso sia remunerato, trattandosi di un contratto di prestazione di servizi o di prestazione d'opera da parte del fornitore, che impiega di norma forza propria per erogarlo.

Tuttavia, lo Stato potrebbe decidere di offrire gratuitamente un servizio soprattutto quando ne impone un obbligo, quando ritiene, cioè, che quel servizio sia essenziale per il benessere della popolazione o per il corretto funzionamento della società, abbia cioè una funzione necessaria o sia di pubblica utilità. In questi casi, lo Stato ritiene che il costo del servizio sia inferiore ai benefici che esso apporta alla collettività. Si veda ad esempio il servizio di conservazione digitale gratuito delle fatture elettroniche offerto dall'Agenzia delle Entrate in virtù dell'utilizzo dell'infrastruttura di Sogei, dopo che è stato introdotto l'obbligo della fatturazione elettronica.

E proprio nel Regolamento 2024/1183 viene fatta una valutazione analoga nel considerando n. 20 del Regolamento stesso con riferimento alla possibilità offerta di avere disponibile, all'interno del digital wallet o portafoglio digitale, l'uso gratuito di una firma elettronica qualificata per tutte le persone fisiche, a fini non professionali.

2. Il panorama dei servizi fiduciari qualificati e non alla luce del nuovo regolamento 2024/1183

Il nuovo Regolamento 2024/1183 che aggiornerà il precedente Regolamento UE n° 910/2014 è inutile negarlo è catalizzato sul tema del digital identity wallet non trascurando tuttavia le evoluzioni in genere legate anche ad altri servizi fiduciari.

Il nuovo schema del regolamento eIDAS ha visto la sua approvazione quale frutto del negoziato interistituzionale informale del trilogo, che riunisce rappresentanti del Parlamento europeo, del Consiglio dell'Unione e della Commissione Europea. In questo articolo si analizza ed approfondisce soprattutto una delle novità proposte nel sopra citato schema "*che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea*", in

particolare quello dell'archiviazione elettronica.

Uno dei principali scopi del Regolamento eIDAS è quello di facilitare le transazioni elettroniche ed il mercato permettendo di effettuare operazioni in modo sicuro. Ogni transazione, di qualunque genere sia, di fatto genera dati che aggregati nelle diverse forme divengono documento informatico, anch'esso da tutelare. Con il nuovo regolamento si assiste ad un'evoluzione... quanto previsto fino ad ora non basta più, non è più sufficiente a garantire le transazioni elettroniche e le persone poste al centro della transazione, in quanto soggetti attivi protagonisti. Va tutelata la persona, i suoi dati, favorite le transazioni sicure e tutelati i documenti e dati informatici generati dalle stesse.

Il considerando numero 4 del Regolamento riprende infatti la "dichiarazione europea sui diritti e i principi digitali per il decennio digitale", proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione ("dichiarazione"), e sottolinea *il diritto di ogni persona di avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione. Ciò include la garanzia che a tutte le persone che vivono nell'Unione sia offerta un'identità digitale accessibile, sicura e affidabile che dia accesso a un'ampia gamma di servizi online e offline, protetti contro i rischi di cibersicurezza e la criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità. La dichiarazione stabilisce inoltre che ogni persona ha diritto alla protezione dei propri dati personali. Tale diritto comprende il controllo su come i dati sono utilizzati e con chi sono condivisi.*

L'obbiettivo del Regolamento va dunque nella direzione di dilatare l'interoperabilità e l'integrazione dei servizi fiduciari nell'Unione Europea, focalizzandosi sulla possibilità di gettare le basi per la creazione di un mercato unico digitale europeo. Il nuovo Regolamento esprime fortemente la necessità all'interno dello scenario comunitario di individuare un'armonizzazione tra i servizi fiduciari ed i servizi fiduciari qualificati. Questo, tuttavia, nell'autonomia degli Stati membri che, come recita lo stesso Regolamento,

"In relazione ai servizi di archiviazione elettronica non armonizzati dal presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni nazionali, in conformità del diritto dell'Unione, relative a tali servizi, quali disposizioni specifiche per i servizi integrati in un'organizzazione e utilizzati esclusivamente per gli archivi interni di tale organizzazione."

Resta tuttavia salvo il principio dell'Unione di tutelare e risolvere l'esigenza di ottenere senza problemi il riconoscimento giuridico della circolazione dei "documenti elettronici". Il Regolamento Europeo in quanto norma di grado superiore, immediatamente applicabile negli Stati membri, rappresenta l'indicazione base su cui strutturare le legislazioni dei singoli paesi membri, una sorta di "linee guida" a cui è necessario attenersi per creare un'unità di visione e di operatività nell'ambito dei servizi fiduciari.

Il nuovo Regolamento rappresenta un passo avanti significativo per l'Europa in materia di identità digitale e servizi fiduciari. Il regolamento mira a creare un

ecosistema digitale più sicuro e interoperabile, offrendo ai cittadini e alle imprese una maggiore scelta e flessibilità nell'utilizzo di servizi online. I servizi fiduciari attualmente previsti dalla vigente versione del Regolamento abbiamo visto essere i servizi di creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche e i servizi elettronici di recapito certificato ed i certificati relativi a tali servizi; i servizi di creazione, verifica e convalida certificati di autenticazione di siti web; i servizi di conservazione di firme; sigilli o certificati elettronici relativi a tali servizi.

Le novità introdotte dal nuovo regolamento vanno analizzate nell'ottica di esaminare le loro implicazioni ed i cambiamenti più rilevanti che comporteranno nell'ecosistema dei servizi fiduciari.

Per quanto riguarda le implicazioni certamente si assiste ad una maggiore attenzione della protezione dei dati personali, ad un potenziamento dei livelli di sicurezza informatica, ad un'attenzione verso la tutela della proprietà dei dati oltre che alla volontà di garantire un accesso sicuro ai servizi pubblici e alle transazioni online in Europa, per tutti i cittadini, i residenti e le imprese dell'Unione.

Tra gli obbiettivi si rilevano la volontà di:

- offrire soluzioni di identità elettronica altamente sicure e affidabili
- garantire che i servizi pubblici e privati possano contare su soluzioni affidabili e sicure di identità digitale
- assicurare che le persone fisiche e giuridiche abbiano la facoltà di utilizzare soluzioni di identità digitale
- fare in modo che tali soluzioni siano legate a una serie di attributi e consentano la condivisione mirata di dati di identità limitati alle esigenze del servizio specifico richiesto
- consentire l'accettazione di servizi fiduciari qualificati nell'UE nonché parità di condizioni per la loro prestazione.

Tra i nuovi servizi fiduciari proposti si rilevano: la gestione degli attributi elettronici, l'archiviazione elettronica, la gestione di dispositivi di firma remota e sigilli, il servizio fiduciario dei registri elettronici distribuiti.

La centralità e l'importanza di tali servizi ritenuti strategici per il futuro dell'Unione è ripreso anche da un altro filone legislativo, quello delle Direttive NIS (1 e 2), che si occupano di sicurezza delle reti e dei sistemi informativi nell'Unione.

Tutti i soggetti che operano in specifici settori ritenuti essenziali per i paesi membri – gli Operatori di Servizi Essenziali (OSE) e i Fornitori di Servizi Digitali (FSD) devono innalzare e uniformare i loro livelli di sicurezza: da un lato affidandosi a fornitori certificati per le proprie architetture digitali, dall'altro sottostando a precisi obblighi di notifica in caso di incidenti o attacchi informatici.

In particolare, la Direttiva NIS 2 (o Direttiva UE 2022/2555)[1] aggiunge all'elen-

[1] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555

co dei soggetti già inclusi nella sua precedente versione (Direttiva NIS 1 del 2016, adottata in Italia con il D.L. n.65 del 18 maggio 2018) proprio quegli stessi prestatori di servizi fiduciari definiti dal regolamento eIDAS. L'aggiunta di nuovi servizi all'elenco di quelli già considerati come "fiduciari" estende dunque l'ambito di applicazione della Direttiva NIS 2, includendo ulteriori soggetti tenuti a innalzare e rivedere i propri standard di cybersecurity e a rispettare stringenti obblighi di segnalazione in caso di incidente. Tutti questi servizi dovranno rispettare specifici standard di cybersecurity (richiesti dalle Direttive NIS) per gestire i rischi di sicurezza informatica e ridurre gli eventuali impatti che si potrebbero avere su cittadini e imprese nell'erogazione dei servizi stessi e tale previsione riguarda sia i servizi fiduciari qualificati che i servizi fiduciari.

Il considerando 47 al nuovo Regolamento prevede infatti : … *Nel fissare le condizioni alle quali i quadri fiduciari dei paesi terzi potrebbero essere considerati equivalenti ai quadri fiduciari per i servizi fiduciari qualificati e i relativi prestatori ai sensi del regolamento (UE) n. 910/2014, è opportuno garantire il rispetto delle pertinenti disposizioni di cui alla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio13 e al regolamento (UE) 2016/679, nonché l'uso di elenchi di fiducia quali elementi essenziali per costruire la fiducia.*

Il regolamento esplica bene come i servizi fiduciari possono essere qualificati o non qualificati. Questi ultimi pur non essendo soggetti agli stessi requisiti dei servizi qualificati e non essendo caratterizzati da alcune presunzioni forti che caratterizzano i servizi fiduciari qualificati, devono tuttavia offrire comunque un elevato livello di sicurezza e affidabilità.

Il considerando 50 al Regolamento prevede infatti:

Al fine di razionalizzare gli obblighi in materia di cibersicurezza imposti ai prestatori di servizi fiduciari, nonché di consentire a tali prestatori e alle rispettive autorità competenti di beneficiare del quadro giuridico istituito dalla direttiva (UE) 2022/2555, a norma di tale direttiva i servizi fiduciari sono tenuti ad adottare misure tecniche e organizzative adeguate, quali misure per far fronte a guasti del sistema, errori umani, azioni malevole o fenomeni naturali, per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare minacce informatiche e incidenti significativi conformemente alla medesima direttiva.

I servizi fiduciari qualificati, di contro, ed i prestatori di servizi fiduciari qualificati (QTSP) che offrono tali servizi devono soddisfare requisiti rigorosi in termini di sicurezza, affidabilità e conformità offrendo un livello di garanzia più elevato.

Non di meno i considerando 44 e 45 al regolamento prevedono la volontà di instaurare anche un regime sanzionatorio rigido a tutela della corretta applicazione delle previsioni regolamentari da parte dei prestatori di servizi fiduciari ed infatti prevedono:

(*44) Al fine di garantire l'efficace applicazione del presente regolamento, è opportuno stabilire un limite minimo per il livello massimo di sanzioni amministrative per i prestatori di servizi fiduciari sia qualificati che non qualifi-*

cati. Gli Stati membri dovrebbero prevedere sanzioni effettive, proporzionate e dissuasive. Nel determinare le sanzioni è opportuno tenere debitamente conto delle dimensioni dei soggetti interessati, dei loro modelli di business e della gravità delle violazioni.
(45) Gli Stati membri dovrebbero stabilire norme relative alle sanzioni applicabili a violazioni quali le pratiche dirette o indirette che generano confusione tra servizi fiduciari non qualificati e servizi fiduciari qualificati o l'uso abusivo del marchio di fiducia UE da parte di prestatori di servizi fiduciari non qualificati. Il marchio di fiducia UE non dovrebbe essere utilizzato in condizioni che, direttamente o indirettamente, inducano a ritenere che i servizi fiduciari non qualificati offerti da tali prestatori siano qualificati.

Vedremo in seguito come questo potrà anche influire sulle attuali dinamiche di mercato.

3. Dalla conservazione all'e-archiving

Per affrontare coerentemente il passaggio dalla conservazione digitale all'e-archiving è opportuno analizzare: cosa cambia, come cambia, quali impatti ha il cambiamento e soprattutto quali sono gli effetti legali di questo passaggio.

I processi conservativi presentano un'elevata complessità sia per la pluralità delle forme di produzione dei contenuti digitali da parte delle organizzazioni e delle persone sia per la differenziazione delle modalità di rappresentazione digitale e di condivisione e trasmissione, ma anche per la presenza di numerosi standard tecnici specifici.

La conservazione a lungo termine dei contenuti digitali è un processo che deve partire dalla fase della loro formazione al fine di assicurarne in modo sostenibile e accurato l'autenticità, l'affidabilità e l'accesso nel tempo. Attualmente l'Art. 44 1-ter CAD (Codice dell'Amministrazione Digitale – Dl.gs 82/2005 e successive modifiche ed integrazioni)[2] prevede che il sistema di conservazione dei documenti informatici assicuri, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee guida. Il Glossario (Allegato 1) delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici[3] definisce la 'conservazione' come "*l'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti*".

[2] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82

[3] https://www.agid.gov.it/it/linee-guida

Per arrivare a regole comuni tra Europa e Italia è indispensabile comprendere quanto stabilito nel testo del regolamento 2024/1183 al fine di analizzare compiutamente i concetti di archiviazione elettronica e del relativo servizio qualificato o non qualificato.

A supporto di questa esplicazione devono essere prese in considerazione le constatazioni riportate nei considerando 66 e 67 del Regolamento stesso, che riprenderemo parzialmente anche in seguito e che suggeriscono un allineamento procedurale in merito all'archiviazione ispirandosi al quadro giuridico degli altri servizi fiduciari già contemplati dal Regolamento.

I considerando prevedono infatti:

(66) Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione elettronica sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e documenti elettronici, nonché per i servizi fiduciari associati. Al fine di garantire la certezza giuridica, la fiducia e l'armonizzazione in tutti gli Stati membri, è opportuno istituire un quadro giuridico per i servizi di archiviazione elettronica qualificati, ispirato al quadro per gli altri servizi fiduciari di cui al presente regolamento. Il quadro giuridico per i servizi di archiviazione elettronica qualificati dovrebbe offrire ai prestatori di servizi fiduciari e agli utenti un pacchetto di strumenti efficiente che comprenda requisiti funzionali per il servizio di archiviazione elettronica, nonché chiari effetti giuridici in caso di utilizzo di un servizio di archiviazione elettronica qualificato. Tali disposizioni dovrebbero applicarsi ai dati elettronici e ai documenti elettronici creati in forma elettronica e ai documenti cartacei che sono stati scannerizzati e digitalizzati. Ove necessario, tali disposizioni dovrebbero consentire che i dati elettronici e i documenti elettronici conservati siano trasferiti su supporti o formati diversi al fine di estenderne la durabilità e la leggibilità oltre il periodo di validità tecnologica, evitando nel contempo, nella misura del possibile, le perdite e le alterazioni. Quando i dati elettronici e i documenti elettronici trasmessi al servizio di archiviazione elettronica contengono una o più firme elettroniche qualificate ovvero uno o più sigilli elettronici qualificati, il servizio dovrebbe utilizzare procedure e tecnologie in grado di estendere la loro affidabilità per il periodo di conservazione di tali dati, eventualmente ricorrendo all'uso di altri servizi fiduciari qualificati istituiti dal presente regolamento. Per la creazione delle prove di conservazione in caso di utilizzo di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, è opportuno utilizzare servizi fiduciari qualificati. In relazione ai servizi di archiviazione elettronica non armonizzati dal presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni nazionali, in conformità del diritto dell'Unione, relative a tali servizi, quali disposizioni specifiche per i servizi integrati in un'organizzazione e utilizzati esclusivamente per gli archivi interni di tale organizzazione. Il presente regolamento non dovrebbe distinguere tra dati elettronici e i documenti elettronici creati in forma elettronica e docu-

menti fisici che sono stati digitalizzati.
(67) Le attività degli archivi nazionali e delle istituzioni della memoria, in qualità di organizzazioni preposte alla conservazione del patrimonio documentario nell'interesse pubblico, sono generalmente disciplinate dal diritto nazionale e non forniscono necessariamente servizi fiduciari ai sensi del presente regolamento. Nella misura in cui tali istituzioni non forniscono tali servizi fiduciari, il presente regolamento non ne pregiudica il funzionamento.

Non di minore rilevo risultano poi le definizioni contenute nei punti 48) e 49) a modifica dell'articolo 3 del Regolamento che individuano in maniera precisa gli obbiettivi che il servizio di archiviazione elettronica deve raggiungere.

Il punto 48 recita infatti:

48) "archiviazione elettronica", un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione;

Si nota immediatamente come vi sia una grande attenzione ad alcuni concetti essenziali già presenti nella normativa italiana sia con riferimento alla gestione documentale che alla conservazione: reperibilità del documento, fruibilità, gestione dello scarto documentale, leggibilità, mantenimento del suo valore probatorio, integrità, riservatezza, origine ed autenticità.

Il punto 49 invece fa riferimento al servizio fiduciario qualificato ed in particolare:

49) "servizio di archiviazione elettronica qualificato", un servizio di archiviazione elettronica fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 undecies;

Riprendendo l'articolo 45 undecies, lo stesso prevede e chiarisce oggettivamente i requisiti per i servizi di archiviazione elettronica qualificata così definiti:

Articolo 45 undecies Requisiti per i servizi di archiviazione elettronica qualificati

1. I servizi di archiviazione elettronica qualificati soddisfano i requisiti seguenti:

a. sono forniti da prestatori di servizi fiduciari qualificati;
b. utilizzano procedure e tecnologie in grado di garantire la durabilità e la leggibilità dei dati elettronici e dei documenti elettronici oltre il periodo di validità tecnologica e almeno per tutto il periodo di conservazione legale o contrattuale, preservandone nel contempo l'integrità e l'esattezza dell'origine;
c. assicurano che tali dati elettronici e tali documenti elettronici siano con-

servati in modo tale da essere protetti dal rischio di perdita e alterazione, ad eccezione delle modifiche riguardanti il loro supporto o il loro formato elettronico;

d. *consentono alle parti autorizzate facenti affidamento sulla certificazione di ricevere una relazione in un modo automatizzato in cui si conferma che i dati elettronici e i documenti elettronici consultati da un archivio elettronico qualificato godono della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento della consultazione.*

La relazione di cui alla lettera d) del primo comma è fornita in modo affidabile ed efficiente e reca la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore del servizio di archiviazione elettronica qualificato.

Inoltre, il secondo comma prevede che:

2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai servizi di archiviazione elettronica qualificati. Si presume che i requisiti dei servizi di archiviazione elettronica qualificati siano rispettati ove un servizio di archiviazione elettronica qualificato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

Questo secondo comma è tutt'altro che trascurabile richiamando la presunzione forte che i requisiti dei servizi di archiviazione elettronica qualificati siano rispettati ove un servizio di archiviazione elettronica qualificato adempia dette tali norme, specifiche e procedure e richiamando ad atti di esecuzione che dovranno essere adottati entro 12 mesi. È d'uopo una riflessione in tema di standard e norme attualmente adottate nella gestione dei sistemi di conservazione a norma in Italia, più innanzi approfondita nel paragrafo 5 di cui infra.

Si rileva rilevante, inoltre, in tema di interoperabilità di servizi di archiviazione elettronica qualificata quanto previsto dall'art. 24 bis comma 10

10. Un servizio di archiviazione elettronica qualificato fornito in uno Stato membro è riconosciuto quale servizio di archiviazione elettronica qualificato in tutti gli altri Stati membri.

In questo modo l'interoperabilità dei servizi e la loro portabilità è garantita, ma quale sarà l'impatto sul mercato?

Proseguendo la nostra analisi possiamo vedere come nel Regolamento eIDAS attualmente vigente, il concetto di e-archiving invece praticamente non esiste: si parla solamente di Qualified preservation service for qualified electronic signatures

(art. 34)[4], vale a dire un servizio prettamente tecnico, cioè un servizio fiduciario qualificato capace di estendere l'affidabilità delle firme qualificate oltre la loro validità tecnologica, superandone cioè l'obsolescenza. È un servizio inevitabilmente qualificato da una forte connotazione tecnologica e crittografica, ma che non ha avuto un grande ritorno di mercato al netto di una sua diffusione sia in termini di prestatori che di servizi erogati concentrati principalmente nei Paesi dell'Est Europa. A onor del vero è necessario evidenziare come un paio di provider italiani, abbiamo tentato di qualificarsi per tale servizio in Italia ma stante l'impossibilità di farlo abbiano preferito ricorrere a branch ubicate in paesi stranieri in grado di erogare il servizio in oggetto. Il merito del nuovo regolamento eIDAS va finalmente nella direzione di aver colto l'importanza del dato e del documento accostando a questo servizio di signature preservation, un servizio di electronic archiving. Fondamentale è infatti quanto sopra riportato con il considerando 66.

Se partiamo dall'assunto che la Conservazione ho come scopo quello di tutelare la memoria storica dell'informazione e mantenere inalterato il valore probatorio del documento, comprendiamo perché finalmente anche a livello europeo hanno perfettamente compreso che non era più sufficiente mantenere inalterato solo il valore probatorio della firma ma diventava indispensabile custodire l'oggetto informatico. Semplificando al massimo il tema, la conservazione è una custodia ordinata di un bene finalizzata a prevenire sia alterazioni naturali della cosa, sia danneggiamenti o sottrazione da parte di terzi, sia ancora violazioni dello stato giuridico del bene e trattandosi di un bene informatico si cerca di mantenerne inalterate le caratteristiche strutturali che aveva al momento della sua formazione, organizzando il tutto in un archivio informatico gestito secondo le logiche archivistiche da tempo note, in grado di garantire la costante fruibilità del documento nel tempo oltre a mantenere inalterato il suo valore probatorio. È interessante come a livello europeo si sia compreso che si tratta di un servizio rilevante e quindi e-archiving sia stata annoverata tra i servizi fiduciari prevedendo per gli stessi prestatori di servizi fiduciari qualificati e non il rispetto dei requisiti stabiliti nel regolamento stesso oltre che nell'articolo 21 della direttiva (UE) 2022/2555. Altrettanto rilevante è analizzare gli effetti legali dell'eArchiving previsti dall'art. 45 decies della bozza di Regolamento.

Nello specifico con riferimento alla portata giuridica dei servizi di archiviazione elettronica si prevede che:

1. *Ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.*
2. *I dati elettronici e i documenti elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della presunzione della*

[4] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN#d1e1772-73-1

loro integrità e della correttezza della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato.

Si ricavano alcuni principi essenziali tipici del Regolamento eIDAS: non discriminazione, per un servizio qualificato presunzione di integrità e di origine per la durata del periodo di conservazione, portabilità. Inoltre, si evidenzia come con riferimento all'archiviazione si disciplinino sia i dati che i documenti.

A tal fine non è trascurabile anche la proposta Agid di Linee Guida in relazione alla conservazione di una base di dati che rappresenta sia una struttura logica di memorizzazione sia uno strumento per la gestione dei dati e delle loro associazioni.

Non sarà semplice definire le regole di e-archiving inerenti ai dati poiché è necessario mantenere i dati anche successivamente alle eventuali integrazioni o modifiche, oltre alla capacità di memorizzare le interazioni tra utenti, sistemi e dati e di preservare da sovrascrittura sia i dati che le informazioni sulle interazioni e quindi conservare una struttura dinamica. Sarà indispensabile definire regole per l'estrazione, in una forma statica, dei dati memorizzati e tenere presenti le soluzioni tecniche in grado di garantire l'accesso nel tempo alle informazioni, mantenendone l'integrità e l'autenticità.

L'armonizzazione normativa tra Italia ed Europa sarà determinante per questo servizio. Attualmente l'Agenzia per l'Italia Digitale definisce le modalità operative per realizzare l'attività di conservazione indicando la natura e funzione del sistema, i modelli organizzativi; i ruoli e funzioni dei soggetti coinvolti; la descrizione del processo di conservazione ed i profili professionali dei responsabili impiegati nel processo di conservazione. L'approccio comunitario e quello nazionale hanno componenti operative sovrapponibili ma fondamentale sarà definire regole chiare per evitare contraddizioni tra norme comunitarie e nazionali, evitare equivoci che possano portare gli operatori verso procedure di infrazione e sanzioni, interagire attivamente con l'organismo di standardizzazione al fine di definire regole tecniche da armonizzare con la situazione nazionale esistente. Il nuovo servizio fiduciario di e-archiving ha un impatto sulla conservazione nazionale dei documenti informatici che deve essere gestito opportunamente, anche aggiornando le norme nazionali, per evitare disparità tra soggetti nazionali e comunitari (si pensi ai 5 milioni di euro di capitale sociale richiesti per ottenere la qualifica in Italia che rappresentano una barriera di ingresso rispetto ai soggetti qualificati nell'Unione), ma anche per mantenere l'equilibrio tra norme nazionali, che hanno scopi specifici per il patrimonio documentale pubblico e norme europee che essendo di rango normativo superiore non possono essere messe a rischio sul tema della applicabilità da norme nazionali non conformi a quelle comunitarie e quindi abrogate de jure.

4. I requisiti che un fornitore di servizi fiduciari di e-archiving deve possedere

Per diventare un'azienda in grado di erogare servizi fiduciari è necessario possedere determinati requisiti.

I servizi fiduciari qualificati sono sottoposti alla vigilanza di appositi organismi governativi nazionali, in Italia l'AgID – l'Agenzia per l'Italia Digitale. Di norma per l'Italia i soggetti che vogliono fornire servizi fiduciari qualificati o svolgere attività di gestione di posta elettronica o d'identità digitale, devono presentare all'AgID una domanda di qualificazione, la quale deve essere conforme alle regole e alle modalità fissate dalle Linee guida. I prestatori di servizi fiduciari qualificati sono autorizzati a caratterizzare il servizio qualificato offerto attraverso l'uso del marchio di fiducia UE per i servizi fiduciari qualificati. Tale marchio di fiducia è regolamentato dal Regolamento di esecuzione (UE) 2015/806 della commissione del 22 maggio 2015. L'AgID, ai sensi dell'art. 14-bis, comma 2, lettera i) del Codice dell'Amministrazione Digitale (CAD – Decreto legislativo 7 marzo 2005, n. 82, s.m.i.) esercita funzioni di vigilanza sui prestatori di servizi fiduciari qualificati in materia di identificazione elettronica e trusted services, ai sensi dell'articolo 17 del regolamento UE 910/2014 oltre che sui gestori di posta elettronica certificata e sui soggetti di cui all'articolo 34, comma 1-bis, lettera b), nonché' sui soggetti, pubblici e privati, che partecipano a SPID di cui all'articolo 64, il tutto al fine di prevenire irregolarità, malfunzionamenti o disservizi nei processi di erogazione e per verificare che i soggetti vigilati operino nel rispetto di regole e requisiti definiti e mutuamente riconosciuti tra agli Stati Membri dell'Unione Europea, con l'obiettivo di rafforzare la fiducia dei cittadini nelle transazioni on line e favorire lo sviluppo dell'economia digitale. In questa sua attività Agid mira altresì ad accertare presunte violazioni da cui possono derivare utilizzi impropri o a scopo fraudolento dei predetti servizi, esponendo l'utente al rischio di falsificazioni o di furti di dati.

Per tali finalità, l'Agenzia, nel suo ruolo di autorità di vigilanza, svolge accertamenti di tipo ispettivo e promuove verifiche in via preventiva, in un'ottica di miglioramento continuo dei processi per la qualità e la sicurezza dei servizi. Con riferimento all'e-archiving abbiamo visto come l'art. 45 undecies delle bozze di Regolamento presenta una prima lista di requisiti che il Qualified Trust Service Provider deve possedere per erogare il servizio di qualified archiving. Questo posiziona a tutti gli effetti i servizi di conservazione digitale attualmente intesi tra i Trust Service, cioè tra i servizi fiduciari che possono essere qualificati, al pari delle firme digitali, delle marche temporali, dei sigilli elettronici.

Del resto, questo era stato inizialmente intuito anche da AgID con i primi accreditamenti dei Conservatori, ai sensi dell'articolo 34 del CAD, articolo poi modificato in virtù del Decreto Semplificazione (D.L. 76/2020), convertito con Legge n. 120/2020, che ha apportato numerose modifiche al Codice dell'amministrazione digitale (CAD) stesso, tra cui alcune relative al servizio di conservazione dei documen-

ti informatici e che ha portato alla emanazione del Regolamento sui criteri per la fornitura di servizi di Conservazione. La conservazione dei documenti informatici per conto delle pubbliche amministrazioni da parte di soggetti esterni deve uniformarsi – nel rispetto della disciplina europea – alle Linee guida sulla formazione, gestione e conservazione dei documenti informatici nonché al sopradetto Regolamento, adottati entrambi dall'Agenzia per l'Italia digitale (AgID), che segnano il superamento del precedente meccanismo di accreditamento dei conservatori. L'emanazione del Regolamento composto con i relativi allegati sui criteri per la fornitura dei servizi di conservazione dei documenti informatici prevede l'istituzione di un elenco (marketplace) per i servizi di conservazione pubblicato su conservatoriqualificati.agid.gov.it dove possono iscriversi i soggetti, pubblici e privati, che intendono erogare il servizio di conservazione dei documenti informatici per conto delle pubbliche amministrazioni.

L'iscrizione al marketplace non è obbligatoria ma i conservatori che intendono partecipare a procedure di affidamento da parte delle pubbliche amministrazioni, a partire dal primo gennaio 2022, data di entrata in vigore del Regolamento, devono ugualmente possedere i requisiti previsti dal Regolamento stesso e sono sottoposti all'attività di vigilanza di AgID.

Tutto questo quindi per evidenziare come in Italia si sia sempre avuto una spiccata sensibilità in relazione ai requisiti che un prestatore di servizi di conservazione deve possedere, a maggior ragione, se fornisce i suoi servizi ad una struttura della Pubblica amministrazione.

È inoltre essenziale rilevare come per quanto riguarda gli altri requisiti previsti dal Regolamento , la garanzia di data/ora certa dell'archiviazione, la produzione di report, il mantenimento di integrità, reperibilità, leggibilità a lungo termine al fine di contrastare l'obsolescenza tecnologica siano da anni la quotidianità dei Conservatori italiani, che in Europa sono certamente tra i soggetti con maggior esperienza e know-how nel settore, sia da un punto di vista temporale (si pensi che la prima deliberazione dell'allora CNIPA sul tema risale al 2004) che da un punto di vista quantitativo in relazione agli oggetti già conservati.

In Italia l'argomento dell'archiviazione elettronica è trattato nell'ambito della formazione, gestione e conservazione dei documenti informatici ed ha una grande rilevanza sia per la pubblica amministrazione, che per i cittadini e le imprese. Ma anche a livello europeo è considerato rilevante, infatti, riprendendo il considerando 66 alla bozza di Regolamento recita (tradotto): "*Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione elettronica sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e documenti elettronici, nonché per i servizi fiduciari associati. ……..*

La lettura del testo comunitario anche più sopra riportato evidenzia l'uso della definizione di archiviazione elettronica coma analoga a quella di conservazione. Sul sito dell'Agenzia per l'Italia Digitale si descrive la conservazione come "l'attività volta a proteggere e custodire nel tempo gli archivi di documenti e dati informatici". L'approccio comunitario e quello nazionale hanno componenti operative sovrap-

poste, quindi è indispensabile definire regole chiare per evitare contraddizioni tra norme comunitarie e nazionali. È importante definire in sede di organismo di standardizzazione, regole tecniche da armonizzare con la situazione nazionale esistente. L'armonizzazione delle regole lato Italia dovrebbe tener conto anche di quanto attualmente previsto per la qualifica dei servizi fiduciari in materia di requisiti aziendali. Come è noto, il capitale sociale minimo per la qualifica previsto dal testo previgente, ma ancora in essere, dell'articolo 29 del CAD è di 5 milioni di euro. Per eliminare questa pericolosa e penalizzante barriera di ingresso alle aziende stabilite in Italia rispetto a quelle nel mercato interno comunitario, le istituzioni nazionali dovrebbe aggiornare le regole di qualifica allineandole con le regole già in uso in altri Stati membri in virtù delle previsioni del Regolamento eIDAS.

5. Gli impatti su un mercato in evoluzione alla ricerca di un'armonizzazione tra normativa italiana e normativa europea

Inevitabilmente si va a configurare un nuovo scenario competitivo. L'introduzione del mutuo riconoscimento tra gli Stati membri, nell'ambito dei servizi di conservazione realizza quello che il primo Regolamento eIDAS ha fatto per le firme qualificate: l'azzeramento delle barriere tra Paesi e un unico singolo mercato europeo comune a tutti. È un cambiamento rilevante dello scenario competitivo che, come sempre, porta con sé rischi ma anche grandi opportunità per il Sistema Paese: l'Italia è da sempre all'avanguardia nella scienza archivistica digitale, anche nella sua implementazione concreta, a supporto dei processi di trasformazione digitale di PPAA e imprese. Questa posizione può consentire la costruzione di campioni nazionali che possano esportare in altri Paesi l'eccellenza archivistica italiana. Al contempo, il digital single market crea un abbassamento delle barriere all'ingresso, consentendo l'arrivo sul mercato domestico di provider stranieri, aumentando il già elevato tasso di competitività sul mercato dell'archiviazione e della conservazione digitale.

Tutto questo va poi collegato alle previsioni normative ed al secondo comma dell'articolo 45 undecies in tema di e-archiving, porta ad una riflessione in tema di standard e norme attualmente adottate nella gestione dei sistemi di conservazione a norma in Italia. Diventa complesso stabilire requisiti nazionali in ambito ETSI e CEN, ma potrebbe essere il momento di separare nelle Linee guida la conservazione privata da quella pubblica, mantenendo SInCRO obbligatorio solo per la seconda ed andando ad amplificare gli aspetti specifici del settore pubblico in tema di conservazione digitale.

Vi è da aggiungere inoltre che i 12 mesi stabiliti nello schema di regolamento non appaiono sufficienti per produrre standard innovativi, sarà quindi necessario gestire al meglio quanto stabilito nel regolamento per gestire la conservazione na-

zionale. L'articolo 45 undecies delle bozze del Regolamento fa riferimento a degli implementing acts per stabilire specifiche tecniche e standard di riferimento, che si spera siano attesi presumibilmente per la fine del 2024, che ci si aspetta siano collegati in qualche modo, per esempio, ai lavori del CEN/TC 468/WG 1 – General concepts for preservation of digital information.

Gli standard di riferimento da cui partire stante l'esiguo periodo previsto dovrebbero essere ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques; ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. Si potrebbe ipotizzare un'evoluzione dell'ETSI TS 119 512 tenendo bene in conto che all'estero, tuttavia, non hanno alcun motivo apparente per mantenere lo status quo dei nostri conservatori e questi documenti devono essere aggiornati poiché sono stati redatti nel contesto del vigente Regolamento eIDAS - articoli 34 e 40. Il nuovo scenario quindi si sovrappone ed allinea a quello vigente. Lo standard 511 è già richiamato nelle normative nazionali, il 512 nell'ottica di armonizzazione con le regole comunitarie deve essere ristrutturato per tutelare quanto già fatto a livello nazionale anche in termini di investimento. Ci sono regole nazionali come l'UNI 11386:2020 (nota come SInCRO – Supporto all'interoperabilità nella conservazione e recupero degli oggetti digitali), sopra citato che definisce tecnicamente le specifiche e le caratteristiche del cosiddetto file di chiusura del pacchetto di archiviazione previsto dallo standard OAIS 14721. Di fatto si tratta di regole che potrebbero allinearsi alle previsioni comunitarie favorendo un principio essenziale quello della portabilità e dell'interoperabilità tra sistemi di conservazione. Alcuni standard e regole potrebbero essere replicati da altri servizi fiduciari (firme e sigilli, marche temporali e servizi elettronici di recapito certificato) prevedendo specifiche regole e norme per lo scambio di documenti e dati tra Stati membri dell'Unione, sfruttando anche quanto previsto in termini di requisiti per i servizi di archiviazione elettronica qualificata in virtù, per esempio, del rapporto automatizzato che conferma che un dato elettronico recuperato da un archivio elettronico qualificato gode della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento del recupero e che tale rapporto deve essere fornito in modo affidabile ed efficiente e recare la firma elettronica qualificata o il sigillo elettronico qualificato del fornitore del servizio di archiviazione elettronica qualificata.

6. Conclusioni verso il futuro che ci attende

Allo stato attuale in tema di e-archiving come evoluzione della conservazione digitale, l'Italia è all'avanguardia e c'è un'opportunità da cogliere e da non lasciarsi sfuggire.

Così come è stato fatto per altri servizi qualificati nel primo Regolamento eIDAS, l'esperienza italiana può risultare determinante in questi momenti decisivi di dialogo, evoluzione ed impostazione di standard e normativa a corredo. Bisogna farsi trovare pronti, sfruttando l'esperienza e la competenza accumulate negli anni nella gestione di un servizio così particolare, per riuscire a governare le decisioni tecniche e il futuro del mercato di questi servizi.

Diventa essenziale agire in maniera compatta e coordinati come sistema Paese nelle interazioni con gli organi regolatori europei e con i partner esteri pubblici ed industriali al fine di valorizzare gli elementi oggettivi che ci vedono leader in questo segmento del digital trust.

In considerazione degli sviluppi in itinere per i servizi di conservazione a norma, per le aziende italiane che vi operano (Conservatori) è essenziale che i requisiti di qualità e sicurezza siano definiti i in modo chiaro e durevole. Vanno considerati e preservati in particolar modo l'alta qualità e il valore aggiunto che sono in grado di offrire oggi i Conservatori italiani grazie alla solida e costante evoluzione delle norme tecniche e all'esperienza maturata. Passando dall'archiviazione elettronica, conservazione "sostitutiva" prima (scansione del cartaceo) e "digitale" ora, è stata introdotta in Italia da ormai quasi trent'anni (dalla lontana Legge Bassanini) una metodologia strutturata e profondamente regolamentata, in tutto il periodo durante il quale l'impianto normativo e tecnologico è stato strutturato, revisionato, arricchito. Negli altri Paesi europei non sussiste al momento un livello analogo di regolamentazione. In particolare, la previsione dell'elenco dei Conservatori Accreditati presso AgID istituito nel 2014 ed ora riqualificato in qualche modo come Marketplace AgID dei servizi di conservazione, con una serie di requisiti puntuali sotto vari profili (sicurezza, organizzazione, competente tecniche ed archivistiche), ha consentito ai Conservatori di sviluppare una competenza estremamente consolidata e verticale attraverso studio, formazione e, non ultimo, un notevole impegno di risorse sia umane che economiche. Se la conservazione con l'e-archiving diviene un servizio fiduciario qualificato significa che debbano valere i requisiti per lo svolgimento dei servizi fiduciari di cui all'art. 29 comma 2 del CAD. E questo indipendentemente da quanto previsto dal Regolamento per il Marketplace dei servizi di Conservazione, che prevede requisiti generali di qualità, di sicurezza e di organizzazione, oltre che specifici profili professionali. Tale articolo richiama tra l'altro i requisiti di cui all'articolo 24 del Regolamento eIDAS, ed in particolare, l'articolo 29, comma 2 del CAD, prescrive nella sua versione attuale che il richiedente la qualificazione e l'accreditamento deve disporre delle garanzie assicurative e di eventuali certificazioni, adeguate rispetto al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. I predetti requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei ministri, sentita l'AgID. DPCM che al fine dell'attuazione compiuta dell'articolo 29 del CAD si auspica venga emanato quanto prima. Tale DPCM, in allineamento alla normativa europea (Regolamento eIDAS) dovrebbe individuare le garanzie di copertura assicurativa adeguate rispetto all'attività svolta, le certificazioni ed i requisiti di onorabilità, affidabilità, tecnologici

e organizzativi compatibili con la disciplina europea che i soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata devono possedere. Nonostante l'emanazione del citato DPCM fosse stata inserita nel programma dei lavori parlamentari del primo semestre 2020, con molta probabilità l'emergenza pandemica di quel periodo ne ha fatto slittare la sua emanazione. Tuttavia poiché a livello europeo (articolo 24 del Regolamento eIDAS) il capitale sociale di per sé non rappresenta un elemento rilevante in relazione alla qualità del servizio fiduciario o all'affidabilità del suo prestatore, non adeguare il predetto articolo 29 comma 2, con il correlativo DPCM potrebbe avere un effetto dirompente nel mercato dei servizi fiduciari con l'avvento del nuovo Regolamento eIDAS ed in particolar modo in quello della Conservazione digitale, con l'effetto di escludere dalla categoria di prestatori di servizi fiduciari qualificati parecchie PMI italiane, che da anni offrono ottimi servizi di conservazione (e che sono state già state precedentemente accreditate e qualificate da AgID sia nell'elenco dei Conservatori Accreditati e poi nel Market Place). Si favorirebbe inoltre l'ingresso sul mercato di società estere con capitale sociale consistente, a prescindere dall'effettiva competenza ed esperienza nel preservare gli archivi informatici. Ma è davvero questo che si vuole? A tutti i livelli è necessario farsi sentire, fare pressing affinché si giunga ad una soluzione in grado di tutelare le PMI italiane, che rappresentano un grande patrimonio di know how e imprenditorialità del Made in Italy digitale.

Il nuovo Regolamento eIDAS avrà un impatto significativo sul panorama dei servizi fiduciari: ci sarà un aumento dell'offerta di servizi: l'introduzione di nuovi servizi fiduciari qualificati e la distinzione tra qualificati e non qualificati amplierà l'offerta di soluzioni per le aziende e i cittadini ma anche per la Pubblica Amministrazione.

L'implementazione del nuovo Regolamento eIDAS presenta alcune sfide, come la necessità di adeguare le normative nazionali e la formazione degli operatori. Tuttavia, il nuovo Regolamento offre anche molte opportunità per le aziende e i cittadini di beneficiare di un ecosistema di servizi fiduciari più sicuro, affidabile e interoperabile. Maggiore sicurezza e affidabilità: infatti i requisiti più rigorosi per i QTSP (qualified trust service provider) garantiranno un livello di sicurezza e affidabilità ancora maggiore per i servizi fiduciari qualificati.

Migliore interoperabilità: eIDAS promuove l'interoperabilità tra i servizi fiduciari in Europa, facilitando l'utilizzo transfrontaliero. In aggiunta il Regolamento eIDAS introduce un sistema di supervisione europeo più armonizzato per i QTSP. Il Regolamento rafforza la fiducia nelle transazioni elettroniche e facilita la digitalizzazione dei processi, rappresenta un passo avanti significativo per l'Europa in materia di identità digitale e servizi fiduciari.

Tuttavia, tanti sono gli interrogativi da porsi soprattutto in considerazione anche del fatto che la conservazione, in ambito privato ma anche e soprattutto pubblico, ha un'importanza essenziale più che strategica dovendo garantire la memoria storica del patrimonio informativo. Come si porrà la PA italiana verso il Regolamento? Potrà permettersi di non rispettarlo o dovrà ove necessario, qualora a livello

europeo non vengano adottati in modo adeguato, adottare standard archivistici in grado di tutelare più che compiutamente il patrimonio documentale? Esiste il considerando 67 del Regolamento da tenere in considerazione che prevede:

> (67) *Le attività degli archivi nazionali e delle istituzioni della memoria, in qualità di organizzazioni preposte alla conservazione del patrimonio documentario nell'interesse pubblico, sono generalmente disciplinate dal diritto nazionale e non forniscono necessariamente servizi fiduciari ai sensi del presente regolamento. Nella misura in cui tali istituzioni non forniscono tali servizi fiduciari, il presente regolamento non ne pregiudica il funzionamento.*

È un cambiamento importante di scenario per il mercato ed è un'occasione unica per i provider italiani da sempre tra i più accreditati nell'ambito dell'archivistica digitale a supporto dei processi di transizione digitale della PA e delle imprese, di affermare la propria leadership.

N. 4 - 2024 - pp. 145-163

Le potenzialità di eIDAS 2.0 sui servizi di conservazione digitale: stato dell'arte, impatti tecnologici e prospettive

Enrico Giunta - Federica Marti

Abstract [IT]: Il quadro normativo e di standardizzazione tecnologica relativo ai servizi di conservazione di documenti digitali ha subito e sta subendo, nell'ultimo decennio, una notevole evoluzione, tanto in ambito italiano quanto europeo. Il panorama nazionale, in particolare, ha visto la transizione dal regime di accreditamento dei conservatori al percorso di qualificazione, coordinato dall'Agenzia per l'Italia Digitale (AgID) per lo specifico ambito della conservazione e dall'Agenzia per la Cybersicurezza Nazionale (ACN) nel caso in cui il servizio sia erogato in cloud, circostanza che ha implicato anche modifiche agli schemi implementativi di riferimento. A livello europeo, recenti valutazioni della Commissione hanno portato all'inserimento nel testo del Regolamento eIDAS degli *electronic archiving services* tra i servizi fiduciari qualificati. Tali circostanze impongono una riflessione su impatti tecnologici e prospettive sul mercato italiano ed europeo, nello specifico da parte dei soggetti che erogano i servizi interessati dalle evoluzioni sopra esposte. Il presente contributo si propone di fornire una sintesi dello stato dell'arte sul tema e, sulla base di questo, analizzare i potenziali scenari che si prefigurano per i conservatori.

Abstract [EN]: The regulatory and technological standardization framework related to electronic document preservation services has undergone and is undergoing, in the last decade, a considerable evolution, both in the Italian and European context. The national landscape, in particular, has seen the transition from the accreditation system for Long-term archiving (LTA) services providers to the qualification one, coordinated by AgID (Italian Agency for the Digitization) for the specific preservation scope and by ACN (National Cybersecurity Agency) in case the service is provided in cloud, a circumstance that has also implied changes to the reference implementation schemas. At a European level, recent evaluations by the Commission have led to the inclusion of *electronic archiving services* among qualified trust services in the text of the eIDAS Regulation. These circumstances impose a review of technological impacts and an evaluation of the perspectives on the Italian and European markets, specifically by the service providers interested by the abovementioned evolutions. The purpose of this contribution is to provide a summary of the state of the art on the topic and, on its basis, to explore the potential scenarios that might be foreseen for LTA services providers.

Parole chiave: *electronic archiving services*, eIDAS, conservazione, normative, standard, implementazioni.

Sommario: 1) Introduzione. 2) Il contesto attuale: normative, standard e implementazioni in Europa e in Italia. 3) eIDAS 2.0: le novità nell'ambito dei servizi di *Electronic Archiving*. 4) Prospettive e impatti in ambito Italiano ed europeo.

1. Introduzione

eIDAS 2.0[1] rappresenta la nuova versione del Regolamento n. 910/2014[2], comunemente noto come eIDAS (ovvero *Electronic Identification And trust Services*), che riguarda l'identificazione elettronica e i servizi per le transazioni elettroniche nel mercato interno europeo. Il nuovo Regolamento espande il panorama dei *qualified trust services* introducendone di nuovi, tra cui l'*electronic archiving*.

Il contesto europeo attuale sulla conservazione digitale si compone di modelli e normative diversificati in base alla singola nazione. Vi sono Stati, come la Spagna, in cui è stato adottato lo schema eIDAS per i *Qualified preservation service for qualified electronic signature and seals*[3]: occorre, infatti, tenere in considerazione che tra i servizi qualificati relativi ad eIDAS, esiste già oggi la conservazione qualificata di firme elettroniche e sigilli elettronici e che i fornitori che intendono offrire i propri servizi censiti nella apposita *trusted list* europea devono utilizzare un sistema in linea con lo standard ETSI TS 119 511 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*.

Altri Stati, come l'Italia, si sono focalizzati sull'emanazione di specifici provvedimenti limitati al perimetro nazionale e hanno sviluppato nel corso del tempo un peculiare modello tramite cui impostare il mantenimento a lungo termine dei documenti informatici identificabile quale 'profilo di conservazione'. Tale profilo si basa, principalmente, sullo standard ISO 14721:2012 *Space data and information transfer systems - Open archival information system (OAIS) - Reference model* e sulle regole tecniche mirate all'implementazione dei cosiddetti 'sistemi di conservazione'.

Vi sono, infine, casi come la Francia, in cui sono presenti entrambe le casisti-

---

[1] *Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.* Le citazioni degli articoli del testo di eIDAS 2.0 (regolamento 2024/1183 dell'11 aprile 2024), saranno esplicitate nel prosieguo dell'articolo in lingua inglese.

[2] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.* Le citazioni degli articoli del Regolamento eIDAS, nel prosieguo del testo, saranno esplicitate in lingua italiana.

[3] Da ora in avanti *QPres services*.

che. È possibile la qualificazione come *QPres Providers* di tipo eIDAS, ma è stabilito un quadro normativo, che, partendo dal Codice del Patrimonio culturale francese, consente l'esternalizzazione dei servizi di archiviazione elettronica per mezzo della certificazione NF 461 - *Système d'archivage électronique pour compte de tiers*.

Con eIDAS 2.0 e l'introduzione degli *archiving services* tra i servizi in esso regimentati, si arriverà a un perimetro comunitario uniforme: ciò comporterà l'allineamento in area UE delle regolamentazioni tecniche e degli standard che i diversi Stati dovranno seguire e, di conseguenza, il mutuo riconoscimento dei servizi.

A tal proposito, l'attuale mancanza di indicazioni certe su quelle che saranno le norme implementative dei nuovi requisiti in materia di archiviazione elettronica consente di esporre alcune prime riflessioni limitatamente ai potenziali impatti sullo stato dell'arte nazionale ed europeo.

2. Il contesto attuale: normativa, standard e implementazioni in Europa e in Italia

Il quadro europeo

Nel contesto europeo vigente pre-eIDAS 2.0, non vi sono riferimenti specifici sulla conservazione digitale dei documenti elettronici in Regolamenti o Direttive.

Nella sua prima formulazione, infatti, il Regolamento eIDAS inquadra soltanto l'aspetto della conservazione che impatta i servizi qualificati in esso normati, ovvero la firma elettronica e i sigilli[4].

Nel dettaglio, l'art. 34 *Servizio di conservazione qualificato delle firme elettroniche qualificate* afferma:

1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica.

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

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate rispondano a dette norme[5].

L'articolo 40 *Convalida e conservazione dei sigilli elettronici qualificati* applica le stesse disposizioni a tale tipologia di strumenti[6].

Le norme tecniche richiamate da questi articoli corrispondono a ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*, standard alla base della certificazione come fornitori di uno qualsiasi dei servizi qualificati in eIDAS e a ETSI TS 119 511 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust services providers providing long-term preservation of digital signatures or general data using digital signature techniques,* schema specifico cui adeguarsi per erogare servizi di conservazione qualificati per firme e sigilli[7].

Non tutti gli Stati europei si sono dotati di normativa tale da consentire la qualifica dei prestatori presso lo Stato stesso per tali servizi di *digital preservation*: l'elenco di fiducia curato dalla Commissione Europea[8] reca traccia di *provider* accreditati in Bulgaria, Francia, Germania, Irlanda, Lituania, Malta, Polonia, Repubblica Ceca, Romania, Slovacchia, Spagna e Ungheria.

A titolo esemplificativo, si espongono quindi la prassi adottata e la normativa di recepimento vigenti in Spagna.

La norma nazionale che vige in materia, ovvero la *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza*, che stabilisce i requisiti di dettaglio per l'applicazione del Regolamento eIDAS, consente ai prestatori di servizi con sede entro i propri confini o in altri Stati europei - purché con una stabile organizzazione in Spagna - di ottenere lo status di *QPres Provider.* Tale provvedimento delinea le condizioni di validità e scadenza dei certificati di firma, di revoca e sospensione; le modalità di identificazione e di verifica degli attributi dei titolari di certificati qualificati; gli obblighi e le responsabilità dei fornitori (comprese quelle inerenti alla trattazione di dati personali); infine, definisce l'autorità di controllo e i suoi poteri di vigilanza e sanzionamento.

Per divenire *QPres provider*, dunque, è necessario, in primo luogo sottoporsi ad audit di verifica basato sugli schemi ETSI sopra citati da parte di un organismo

---

[5] Art. 34 Reg. EU 910/2014.

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

[7] Marti Federica, *Disposizioni normative, modelli e strumenti per la conservazione di documenti e archivi digitali in Italia e in Europa: panorama complessivo, casi di studio, analisi comparata e prospettive*, Università di Macerata, <https://hdl.handle.net/11393/297750>, 2022, pp. 13-14.

[8] L'elenco di fiducia è consultabile pubblicamente al link <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home> (ultima consultazione 23/03/2024).

di certificazione (*Conformity Assessment Body* - CAB) accreditato presso ENAC (*Entidad Nacional de Acreditación*, equivalente dell'italiana Accredia).

In particolare, ETSI 119 511 fornisce linee guida sul modello da implementare e sul profilo di conservazione da erogare in linea con un principio di neutralità tecnologica a livello di dettaglio, mentre definisce i requisiti minimi generali e di contesto. In questo senso, lo standard ETSI appena citato dà la possibilità di disegnare e realizzare profili di conservazione non necessariamente aderenti al modello italiano, in quanto lo schema fornito ha requisiti più ampi, che possono essere visti come un soprainsieme del nostro.

Importante per questo standard è che il sistema di conservazione sia dotato di un identificativo univoco esplicitamente dichiarato nella documentazione di servizio nonché associato e presente nelle evidenze di conservazione. Indici XML o altre tipologie di evidenze in formato testuale strutturato possono accogliere una stringa identificativa (*OID – object identifier*) che lega il file generato durante il processo di conservazione al sistema che lo ha prodotto.

Lo standard ETSI TS 119 511, a differenza del quadro regolatorio italiano in materia, consente di operare con più di un profilo di conservazione, al quale va associato, in ogni caso, un OID. Nel contesto italiano il concetto di "profilo di conservazione" risulta difficile da declinare, in quanto è sostanzialmente unico: è basato su linee guida specifiche, sul modello OAIS e sullo standard UNI 11386:2020 *Supporto all' Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali* (SInCRO), costituito e implementato sulla base del concetto di pacchetto informativo e di evidenza di conservazione in formato XML. Potenzialmente, tuttavia, un processo di conservazione può avvenire secondo differenti paradigmi, utilizzando, ad esempio, tecnologie di *hash-tree* che nella concatenazione degli *hash* garantiscono l'integrità del flusso di archiviazione o tramite la notarizzazione delle evidenze attraverso tecnologie *blockchain*.

Il CAB, quindi, redige un report (*Conformity Assessment Report* - CAR) attestante la conformità a ETSI EN 319 401 del fornitore sottoposto a verifica e a ETSI TS 119 511 delle soluzioni adottate e sviluppate. Tale report deve essere inviato, insieme ai documenti operativi del servizio e alla conferma del possesso di adeguata copertura assicurativa[9], al competente organismo di vigilanza, il SEDIA (*Sede Electrónica de la S.E. de Digitalización e Inteligencia Artificial y S.E. de Telecomunicaciones e Infraestructuras Digitales del Ministerio de Transformación Digital*), il quale informa il prestatore di servizi dell'esito positivo o negativo dell'istanza.

In altri casi, i legislatori hanno sì accolto e promosso la possibilità per i for-

[9] La procedura e l'elenco completo della documentazione da allegare all'istanza di richiesta sono esplicitati nel documento ufficiale *Guía de notificación de servicios electrónicos de confianza cualificados y contenidos mínimos del informe de evaluación de la conformidad en el marco del Reglamento (UE) nº 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercad interior y por el que se deroga la Directiva 1999/93/ce (Reglamento eIDAS)* <https://avancedigital.mineco.gob.es/es-ES/Servicios/FirmaElectronica/Documents/GuiaNotificacion.pdf> (ultima consultazione 02/03/2024).

nitori di divenire QTSP (*Qualified Trust Service Provider*) per la conservazione di firme e sigilli, ma, allo stesso tempo, hanno adottato dei propri schemi per vincolare l'ambito più ampio della conservazione digitale, anche in ragione di necessità legate alla gestione dei documenti pubblici (e di alcune categorie di documenti privati) come parte del patrimonio culturale.

Sempre ai fini esemplificativi, si espone il caso francese.

Quest'ultima realtà mostra una un'estrema attenzione al tema degli archivi digitali: la disamina della normativa e degli strumenti sul tema, infatti, evidenzia l'importanza della cultura archivistica nelle scelte intraprese dal governo francese. È significativa, in tal senso, la scelta di affidare agli aggiornamenti del Codice del Patrimonio Culturale[10] la regolamentazione degli aspetti conseguenti alla dematerializzazione degli archivi, dando vita a un *continuum* analogico-digitale e mantenendo la caratteristica di corpus unitario.

Riguardo alla possibilità di esternalizzare i servizi di archiviazione da parte delle Pubbliche amministrazioni, il quadro di riferimento parte sempre dal *Code du Patrimoine*[11]. È previsto, per quanto concerne i requisiti generali, che qualsiasi soggetto privato voglia beneficiare dell'autorizzazione di svolgere attività di *outsourcing* per la Pubblica Amministrazione debba possedere le certificazioni stabilite dalle norme di riferimento. Nello specifico, l'*Arrêté du 4 décembre 2009 précisant les normes relatives aux prestations en archivage et gestion externalisée* individua come riferimenti gli standard OAIS e NF Z42-013 *Archivage électronique - Recommandations et exigences*. Quest'ultimo descrive le misure tecniche e i processi organizzativi da attuare per l'archiviazione dei documenti elettronici, pone particolare enfasi sulla tracciabilità dei processi utilizzati e sui requisiti del sistema in termini di sicurezza e accesso e definisce le clausole necessarie in un contratto di servizio con una terza parte. Tale norma è stata tradotta nello standard ISO 14641:2018 *Electronic document management - Design and operation of an information system for the preservation of electronic documents - Specifications*. Dal punto di vista applicativo, per attestare la conformità alla norma NF Z42-013, è stata rilasciata da AFNOR (*Association française de normalisation*)[12] la certificazione NF 461 - *Système d'archivage électronique pour compte de tiers* che consente alle organizzazioni e alle aziende di

---

[10] *Code du Patrimoine*, approvato con l'Ordonnance n° 2004-178 du 20 février 2004 *relative à la partie législative du code du patrimoine* per la sua parte legislativa, con Décret n° 2011-573 du 24 mai 2011 *relatif à la partie réglementaire du code du patrimoine* (*Décrets en Conseil d'Etat et en conseil des ministres*) e il Décret n° 2011-574 du 24 mai 2011 *relatif à la partie réglementaire du code du patrimoine* (*livres Ier à VI*) per la parte regolamentare. Per la normativa vigente in Francia: Marti Federica, Disposizioni normative, modelli e strumenti per la conservazione di documenti e archivi digitali in Italia e in Europa: panorama complessivo, casi di studio, analisi comparata e prospettive, Università di Macerata, <https://hdl.handle.net/11393/297750>, 2022, pp. 112-123.

[11] Integrato dal Décret n° 2020-733 du 15 juin 2020 *relatif à la déconcentration des décisions administratives individuelles dans le domaine de la culture*. Tale circostanza è ammessa nei casi degli archivi correnti e di deposito, ma non per gli archivi storici (Art. R212-23, *Code du patrimoine,* come da modificazioni del Decreto n. 2020-733).

[12] AFNOR è l'organizzazione che in Francia si occupa di standardizzazione e normazione.

verificare l'aderenza del proprio sistema ai requisiti di NF Z42-013.

Lo schema NF 461, aggiornato alla quarta versione nel gennaio 2024, si compone di una prima sezione dedicata agli aspetti organizzativi del sistema, ovvero inerenti alla politica di archiviazione, alle responsabilità e competenze, all'impianto contrattuale e ai livelli di servizio, alla documentazione di sistema, alla sicurezza logica e fisica, all'architettura funzionale, applicativa, di sistema e di rete, al supporto, al *change management*, alla tracciabilità e ai log, ed, infine, alle evidenze di processo. Seguono delle parti dedicate al processo di conservazione stesso: sono trattati i requisiti necessari alla fase di versamento e alla creazione dei *Submission Information Package*[13], alla fase di conservazione e di gestione degli *Archival Information Packages* (con attenzione particolare sui siti di conservazione, anche nella loro componente fisica, e sull'integrità, interoperabilità e longevità dei dati) e, infine, alla fase di consultazione e restituzione, (con attenzione particolare ai parametri di ricerca e ai privilegi d'accesso). La norma traduce questi requisiti anche in specifici casi d'uso da testare per accertarsi della conformità delle proprie implementazioni.

Le caratteristiche del profilo di conservazione aderente allo standard NF 461 possono essere considerate compatibili con il modello conosciuto in Italia, rafforzato da una particolare attenzione per il processo di scarto, al quale lo schema assegna una serie di requisiti di implementazione, tracciatura ed automazione molto rigorosi, sempre nel rispetto del possibile dialogo con le autorità nel caso di richiesta di autorizzazione di cancellazione di documenti.

Il processo di rilascio dell'autorizzazione consiste, in primo luogo, nell'esecuzione dell'audit di certificazione per lo standard NF 461 sul servizio di conservazione erogato da prestatore di servizi (condizione sufficiente nel caso in cui l'esternalizzazione debba essere effettuata da un privato a favore di altro privato). Una volta in possesso del certificato, il fornitore può inviare la propria istanza al prefetto competente sul territorio, il quale, sentito il direttore degli archivi dipartimentali interessati, è incaricato di emettere il provvedimento di autorizzazione. Restano, comunque, la legittimità dei direttori degli archivi dipartimentali a intervenire nell'ambito del controllo tecnico-scientifico dello Stato sugli archivi[14], in particolare per eventuali visite in loco di ispezione sui documenti oggetto di esternalizzazione e il supporto agli archivisti con i fornitori, in particolare sui termini dei contratti o sulla scelta dell'archiviazione esterna o interna (in Francia o all'estero) in base alla rilevanza degli archivi. È prerogativa del SIAF (*Service Interministériel des Archives de France*) l'aggiornamento delle pagine del portale *FranceArchives*[15] dedicate ai regolamenti, alle condizioni di approvazione e all'elenco aggiornato dei fornitori autorizzati.

---

[13] La denominazione, così come la seguente di *Archival Information Package*, si riferisce al modello OAIS. In proposito si veda il paragrafo dedicato al panorama italiano.

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

[15] Il portale *FranceArchives* è accessibile al link <https://francearchives.fr/fr/> (ultima consultazione 23/03/2024). Questo portale, inoltre, riunisce in un'unica struttura, tutti i siti web degli archivi territoriali, utilizzando il web semantico.

Tornando al più generale contesto europeo, per completare il panorama sulla normativa tangente l'ambito della conservazione digitale, vanno citati – in relazione ai dati conservati – anche il GDPR[16] e il Regolamento UE 2018/1807 sulla libera circolazione dei dati non personali[17]. In secondo luogo, impattano sul tema i provvedimenti sulla sicurezza, quali Cybersecurity Act[18] e la Direttiva NIS[19], recentemente emendata con la Direttiva NIS 2[20], che è richiamata in maniera diretta nelle disposizioni di eIDAS 2.0.

Il panorama italiano

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

Il campo di applicazione relativo alla conservazione dei documenti informatici può essere considerato senza dubbio maturo e dal perimetro definito, anche grazie a riflessioni teoriche ed accademiche che hanno accompagnato il lavoro del legislatore in quasi venti anni. Ciò ha portato all'implementazione di sistemi di conservazione disegnati e sviluppati secondo il quadro normativo e a numerose iniziative di confronto fra gli addetti ai lavori, professionisti del settore, associazioni, archivisti e informatici. La peculiarità e specificità di questo settore in Italia sono testimoniate anche a livello terminologico, con la scelta di utilizzare la definizione "conservazione" piuttosto che archiviazione elettronica.

Il riferimento cardine del perimetro normativo nazionale è costituito dal Decreto Legislativo n. 82 del 2005, il *Codice dell'Amministrazione Digitale*[21]: in questo dispositivo si trovano i riferimenti primari per la conservazione dei documenti informatici, da cui discendono le successive regolamentazioni tecniche e linee guida. Nella prima versione del CAD la modalità prevista per emanare tali provvedimenti è

---

[16] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

[17] *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.*

[18] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[19] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*

[20] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).*

[21] Da qui in avanti CAD.

costituita dai decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie[22], ma, con i D.Lgs. 26 agosto 2016 n. 179[23] e D.Lgs. 13 dicembre 2017[24], viene posta la medesima responsabilità in capo all'Agenzia per l'Italia Digitale, incaricata di produrre apposite linee guida[25]. Con la rimozione, nel 2017, dell'articolo 44-bis sui conservatori accreditati, viene inserito il vincolo di aderenza alle modalità fissate dalle Linee guida per la domanda di accreditamento, che nel 2022 diviene, con l'entrata in vigore di tale provvedimento, qualificazione[26]. Tali modifiche sono state determinate dal passaggio obbligatorio di consultazione in Commissione Europea, previsto dalla Direttiva UE 2015/1535[27]: nello specifico, le modifiche del Decreto-legge 16 luglio 2020 n. 76 *Misure urgenti per la semplificazione e l'innovazione digitale*[28] al CAD hanno implicato un significativo snellimento del processo autorizzativo, nonché una ridefinizione, in ottica maggiormente europea, dei requisiti per ottenere l'iscrizione nel *Marketplace dei conservatori qualificati*[29].

In conformità ai requisiti delle *Regole Tecniche in materia di sistemi di conservazione digitale*[30] – efficaci sino al gennaio 2022 – la Circolare AgID n. 65 del 10 aprile 2014[31] descriveva le modalità dell'iter istruttorio previsto per l'accreditamento, da espletarsi a carico di AgID stessa. È da evidenziare l'obbligo per il conservatore

---

[22] Art. 71 CAD (versione previgente al D.Lgs. 30 dicembre 2010, n. 235).

[23] Decreto legislativo 26 agosto 2016, n. 179 *Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*. Va evidenziato come questa modifica al CAD sia consequenziale all'entrata in vigore del primo Regolamento eIDAS: i fornitori di servizi di conservazione vengono collocati tra i soggetti che, per prestare servizi qualificati, devono rivolgere domanda ad AgID e rispettare le condizioni previste dal Regolamento 910/2014, venendo di fatto accostati ai Trust Service Provider definiti nello stesso Regolamento (art. 29 CAD, versione previgente al D.lgs 13 dicembre 2017, n. 217).

[24] Decreto legislativo 3 dicembre 2017, n. 217 *Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*.

[25] Art. 71 CAD *Regole tecniche* (versione previgente al Decreto Semplificazioni).

[26] Art. 29 CAD *Qualificazione e accreditamento* (versione previgente al Decreto Semplificazioni).

[27] Direttiva (UE) 2015/1535 del Parlamento Europeo e del Consiglio del 9 settembre 2015 *che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*.

[28] Noto come Decreto Semplificazioni.

[29] La piattaforma, aggiornata da AgID, è disponibile al link <https://conservatoriqualificati.agid.gov.it/?page_id=276> (ultima consultazione: 27/03/2024). Per la ricostruzione normativa sul CAD: Marti Federica, *Disposizioni normative, modelli e strumenti per la conservazione di documenti e archivi digitali in Italia e in Europa: panorama complessivo, casi di studio, analisi comparata e prospettive*, Università di Macerata, <https://hdl.handle.net/11393/297750>, 2022, pp. 59-65.

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

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

accreditato di presentare, a partire dalla data di autorizzazione comunicata dall'Agenzia, un certificato di conformità del sistema di conservazione ai requisiti tecnici organizzativi stabiliti, rilasciato da un ente di certificazione accreditato da ACCREDIA: tale circostanza imponeva al conservatore l'emissione di un certificato da parte di un *Conformity Assessment Body* e il sottoporsi alle sue verifiche di sorveglianza.

AgID, a seguito dell'entrata in vigore delle *Linee Guida AgID sulla formazione, gestione e conservazione del documento informatico*[32], ha emesso il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*[33], che contiene i requisiti generali, di qualità, di sicurezza e organizzazione e introduce il *Marketplace per i servizi di conservazione*. Nel Regolamento sono fissate le indicazioni sia per i soggetti pubblici sia privati che erogano soluzioni di conservazione per conto delle Pubbliche amministrazioni: è esplicitato, tuttavia, che l'iscrizione al Marketplace non è obbligatoria, ma che i conservatori che intendono partecipare a procedure di affidamento pubbliche debbano ugualmente possedere i requisiti previsti ed essere sottoposti all'attività di vigilanza di AgID[34].

L'attuale procedura prevede la trasmissione via PEC da parte del richiedente di apposita autodichiarazione di possesso dei requisiti e del proprio Piano di cessazione. AgID provvede a riscontrare il richiedente con istanza di integrazione, con esito positivo o negativo entro trenta giorni dalla verifica formale della documentazione inviata: in ogni caso, è riservato all'Agenzia il diritto di verificare in ogni momento il possesso dei requisiti previsti, secondo le modalità stabilite dal *Regolamento recante le modalità per la vigilanza*[35].

Tale iter, per i fornitori che erogano il servizio in modalità cloud e intendono rivolgersi alle Pubbliche amministrazioni, va effettuato in parallelo alla richiesta di iscrizione al *Catalogo dei servizi Cloud per la PA qualificati - Cloud Marketplace*[36] gestito dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Quanto agli specifici requisiti tecnici e applicativi previsti dalla normativa sopra citata, la conservazione dei documenti informatici si declina in una serie di operazioni volte alla preservazione in ambiente digitale dei contenuti nel tempo.

---

[32] Adottate con Determinazione n. 407/2020 del 9 settembre 2020 e modificate con Determinazione n. 371/2021 del 17 maggio 2021 (da ora in avanti Linee Guida AgID).

[33] Adottato con Determinazione n. 455/2021, il *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*.

[34] Art. 3 *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici*. È importante evidenziare che, all'art. 1 del Regolamento, viene appositamente esclusa la comprensione, tra le casistiche disciplinate dal provvedimento, dei servizi di conservazione a lungo termine disciplinati dal Codice dei Beni Culturali, con le conseguenti attività di vigilanza e sanzionamento.

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

[36] La piattaforma, curata da ACN, è disponibile al link <https://www.acn.gov.it/portale/catalogo-delle-infrastrutture-digitali-e-dei-servizi-cloud/> (ultima consultazione 27/03/2024).

Ad oggi un sistema di conservazione conforme deve consentire di poter gestire un processo strutturato in più fasi e con elementi chiaramente riconoscibili. Il sistema deve rispondere innanzitutto al modello implementativo definito dallo standard ISO OAIS, basato su pacchetti informativi e sulla tripartizione in macro-perimetri di competenza in cui operano il produttore, l'amministrazione e gli utenti. Tale sistema deve inoltre produrre il cosiddetto "file di chiusura" o evidenza di conservazione, denominato PIndex[37], in conformità allo standard UNI SInCRO. I due standard appena citati caratterizzano in maniera specifica la conservazione digitale e, da un punto di vista tecnico e di processo, prevedono che il sistema di conservazione impieghi differenti pacchetti informativi per poter gestire i dati e i documenti: il *Submission Information Package* (SIP, pacchetto di versamento), generato dal *Producer* e contenente i documenti o le aggregazioni da conservare (compresi i metadati che le descrivono), l'*Archival Information Package* (AIP, pacchetto di archiviazione), prodotto dal conservatore quale evidenza dell'avvenuta conservazione e il *Dissemination Information Package* (DIP pacchetto di distribuzione), generato dal conservatore su richiesta degli utenti e contenente i documenti assieme alle evidenze di conservazione.

Il PIndex contenuto nell'AIP rappresenta, in questo processo, il tratto distintivo del modello italiano, in quanto l'evidenza in formato XML deve essere prodotta obbligatoriamente secondo lo schema dello standard UNI SInCRO, firmata o sigillata dal conservatore ed infine marcata temporalmente per assicurarne la datazione. Anche se permangono tuttora difficoltà nel creare una piena interoperabilità tra differenti fornitori[38], dato che gli schemi di generazione dei SIP e DIP sono sostanzialmente "liberi" e a discrezione del singolo conservatore, la struttura dell'indice dell'AIP è pensata per garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità ai documenti conservati.

Dal punto di vista tecnologico, il quadro normativo italiano e nello specifico le Linee Guida AgID descrivono chiaramente le modalità di implementazione degli standard precedentemente citati. L'allegato 2 relativo ai *Formati di file e riversamento* definisce le estensioni che possono essere accettate dal sistema di conservazione. L'elenco amplia ed espande le potenzialità della conservazione italiana rispetto all'elenco dei formati presenti nel precedente DPCM 13 dicembre 2013 (C) allineandosi anche alle più recenti riflessioni accademiche ed internazionali relative ai formati nell'ambito della *digital preservation*[39]. L'allegato 5 *I metadati* fornisce specifici schemi per la metadatazione del documento informatico, del documento

---

[37] *Preservation Index*, come previsto dallo standard SInCRO.

[38] Si veda la riflessione prodotta da AgID nel documento formalizzato nel dicembre 2022 Modelli *di interoperabilità tra sistemi di conservazione*, consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/interoperabilita_aip.pdf> (ultima consultazione 09/03/2024).

[39] Si veda l'elenco redatto dall'associazione *Open Preservation Foundation* "*International Comparison of Recommended File Formats*" consultabile al link <https://docs.google.com/spreadsheets/d/1XjEjFBCGF3N1spNZc1y0DG8_Uyw18uG2j8V2bsQdYjk/edit#gid=605033917> (ultima consultazione 09/03/2024).

amministrativo informatico e delle aggregazioni documentali informatiche (fascicoli e serie), con l'obiettivo di condividere un modello esaustivo per i differenti scenari in ambito di produzione documentale. I metadati sono stati pensati come set di informazioni «che devono accompagnare il ciclo di vita di un documento informatico»[40] e, per lo specifico ambito della conservazione a lungo termine, anche in ottica di interoperabilità tra sistemi di conservazione. Si è passati dall'obbligatorietà di soli cinque metadati indicati nel DPCM 13 dicembre 2013 (C) a diciotto di cui quattordici obbligatori. Tale complessità ha richiesto la pubblicazione di documentazione a corredo dell'allegato 5, al fine di fornire indicazioni sull'implementazione degli schemi alla luce dei differenti possibili scenari applicativi[41].

Il processo di conservazione delineato nella normativa viene completato dalla descrizione del necessario scarto degli oggetti informatici conservati, volto all'eliminazione degli AIP secondo un processo che prevede la generazione di evidenze dell'avvenuta distruzione degli oggetti digitali (rapporti e indici relativi al processo di scarto) e che si pone in linea con i principi della gestione delle fasi di vita di un archivio.

L'implementazione di quello che possiamo chiamare il "profilo di conservazione italiano" ha portato, nel corso degli ultimi anni, ad una capillare diffusione dell'utilizzo dei sistemi e all'esponenziale aumento del volume dei documenti informatici prodotti e conservati ad oggi, sia per l'adempimento di specifici obblighi, sia per i numerosi flussi di integrazione dei servizi a valle di processi, in cui l'elemento conservativo di documenti precedentemente formati si pone come fase finale e spesso trasparente per l'utente. Basti pensare ai flussi automatici di conservazione associati alla gestione di fatture elettroniche, di messaggi PEC, alla generazione, sottoscrizione e firma di contratti, alle evidenze di identificazione di soggetti in contesti di flussi bancari.

---

[40] Si veda il documento *Modelli di interoperabilità tra sistemi di conservazione*, consultabile al link <https://www.agid.gov.it/sites/default/files/repository_files/interoperabilita_aip.pdf> (ultima consultazione 09/03/2024), p. 6.

[41] Si vedano, in proposito, *Vademecum per l'implementazione delle Linee guida sulla formazione, gestione e conservazione dei documenti informatici* (pubblicato da AgID il 3 novembre 2022 e consultabile al link < https://www.agid.gov.it/sites/default/files/repository_files/vademecum_per_limplementazione_delle_linee_guida_sulla_formazione_gestione_e_conservazione_dei_documenti_informatici.pdf> - ultima consultazione 09/03/2024) e *I metadati del documento informatico di natura fiscale e contabile* (pubblicato da AgID il 17 dicembre 2021 e consultabile al link https://www.agid.gov.it/sites/default/files/repository_files/i_metadati_del_documento_informatico_di_natura_fiscale_e_contabile.pdf - ultima consultazione 09/03/2024).

3. eIDAS 2.0: le novità nell'ambito dei servizi di electronic archiving

Il Regolamento, adottato dal Consiglio Europeo il 26 marzo 2024, prevede l'importante aggiunta dell'*electronic archiving* tra i *Qualified trust services* già inclusi nel previgente eIDAS, circostanza che pone rimedio all'assenza di specifiche disposizioni in materia a livello europeo. I Considerando 66 e 67 esplicitano la consolidata consapevolezza della necessità di un quadro giuridico comunitario per il riconoscimento transfrontaliero dei servizi di archiviazione elettronica qualificati e di strumenti condivisi per lo sviluppo funzionale dei sistemi - anche al fine di aprire nuove opportunità di mercato - in quanto molti degli Stati membri possiedono già normativa di settore per la conservazione a lungo termine dei documenti elettronici:

Many Member States have introduced national requirements for services providing secure and trustworthy electronic archiving in order to allow for the long-term preservation of electronic data and electronic documents, and associated trust services. To ensure legal certainty, trust and harmonisation across Member States, a legal framework for qualified electronic archiving services should be established, inspired by the framework of the other trust services set out in this Regulation. The legal framework for qualified electronic archiving services should offer trust service providers and users an efficient toolbox that includes functional requirements for the electronic archiving service, as well as clear legal effects when a qualified electronic archiving service is used[42].

Dunque, vengono introdotte, all'articolo 3, le definizioni di 'archiviazione elettronica' e 'servizio di archiviazione elettronica qualificato':

> (48) "electronic archiving" means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;
>
> (49) "qualified electronic archiving service" means an electronic archiving service which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45j;

Le fasi di *receipt*, *storage*, *retrieval* e *deletion* indicate nel testo descrivono le funzioni minime e necessarie di un servizio di archiviazione elettronica di dati informatici. La genericità di tale processo è, però, vincolata allo scopo dell'archiviazione elettronica che il legislatore europeo intende dare al servizio: garantire la durabilità e la leggibilità nel tempo, preservare l'integrità, confidenzialità e autenticità dei dati. Tali concetti sono approfonditi ulteriormente nella sezione 10, articolo 45j, del Rego-

[42] *Whereas (66) Regulation of the European Parliament and of the council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.*

lamento, dove vengono indicati gli specifici requisiti necessari per poter considerare qualificato un servizio di archiviazione elettronica:

1. Qualified electronic archive services shall meet the following requirements:
   a. they are provided by qualified trust service providers;
   b. they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin; (c) They ensure that the electronic data is preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format;
   c. they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format;
   d. they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.

   The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.

Se nel complesso il perimetro di tale servizio sembra coerente con il profilo di conservazione italiano, il primo requisito potrà avere senz'altro un impatto decisivo sul mercato in Italia, in quanto gli attuali fornitori di servizi di conservazione digitale dovranno obbligatoriamente passare per una fase di qualificazione di tipo eIDAS al fine di essere considerati *Qualified Trust Service Provider* europei. I requisiti b), c), d), pur nella consueta neutralità tecnologica con cui sono formulati i contenuti del Regolamento, forniscono il perimetro entro il quale le soluzioni di *electronic archiving* dovranno muoversi: garantire l'integrità dei documenti e dei dati archiviati nel tempo e produrre un'evidenza tecnologica dell'avvenuta archiviazione, assicurata da una firma elettronica qualificata o da un sigillo elettronico qualificato.

La sezione 10 tratta, inoltre, nel dettaglio gli effetti giuridici per gli *electronic archiving services*. Nello specifico, l'articolo 45i *Legal effect of electronic archiving services*, riconosce che:

1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form or that they are not preserved using a qualified electronic archiving service.
2. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and

of their origin for the duration of the preservation period by the qualified trust service provider.

Tali principi hanno fondamentale portata poiché il primo definisce in maniera assoluta l'ammissibilità come prova in giudizio di un documento in forma elettronica che sia stato conservato tramite un servizio di *electronic archiving* e il secondo estende i confini geografici della validità giuridica – con presunzione di integrità e origine – di un documento conservato presso un servizio qualificato erogato in uno Stato a tutti gli altri.

Fondamentale per le successive riflessioni sugli impatti di eIDAS 2.0, in particolare, è il comma 10 dell'articolo 24a *Recognition of qualified trust services*, il quale recita: *A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.*

4. Prospettive e impatti in ambito italiano ed europeo

Le premesse sopra esposte inducono alla considerazione che, vista la frammentaria situazione delineata nel quadro iniziale, il nuovo eIDAS costituirà un 'anno zero' per tutti i soggetti che operano nel settore della conservazione digitale, in particolare per quelli già attivi in ambito sia nazionale sia europeo: l'inserimento nel testo degli *electronic archiving services* tra i servizi fiduciari qualificati cambierà, infatti, presto il panorama dei modelli di riferimento[43].

È da porre in rilievo, innanzitutto, il riconoscimento reciproco da parte degli Stati membri UE: il nuovo articolo 24a, oltre a costituire un maggiore e più specifico cardine normativo per tutti i servizi – già o ex-novo - inclusi nel Regolamento – costituisce un fondamento di notevole importanza per l'ambito della conservazione digitale. Una volta ottenuto, in un qualsiasi Paese UE, lo status di fornitore di servizi fiduciari qualificati di *electronic archiving*, il *provider* può distribuire – con tutte le garanzie e i vantaggi del caso – il proprio servizio all'interno del perimetro UE.

A livello di impatto sul mercato è importante operare una riflessione relativa ai requisiti aziendali per quei fornitori che attualmente erogano servizi di questo tipo. Ad esempio, la scelta di quale capitale sociale minimo definire potrebbe rappresentare un vincolo per alcuni soggetti operanti sul mercato, le cui dimensioni, ricordiamolo, diverranno europee. Questo implicherà senza dubbio un riassetto delle attuali

[43] Si vedano, in proposito, anche le riflessioni contenute in G. Manca, *Archiviazione elettronica, le regole nell'era di eIDAS 2: come adeguarsi*, «Agenda Digitale», 13 dicembre 2023, disponibile online al sito <https://www.agendadigitale.eu/documenti/archiviazione-elettronica-le-regole-nellera-di-eidas-2-come-adeguarsi/> (ultima consultazione 04/03/2024) e G. Manca, *Nuovo regolamento eIDAS, ecco come cambia l'archiviazione elettronica*, «Agenda Digitale», 13 dicembre 2023, disponibile online al sito <https://www.agendadigitale.eu/documenti/nuovo-regolamento-eidas-ecco-come-cambia-larchiviazione-elettronica/ > (ultima consultazione 09/03/2024).

regole, principalmente sul versante della concorrenza, con nuovi potenziali gruppi aziendali di Paesi diversi in diretta competizione con quelli nazionali. La possibilità che in un primo tempo si generi un gruppo ristretto di *big players* che guidi il mercato europeo dei servizi di *electronic archiving* non è da escludere in questo senso, ma sarà necessario seguire l'evoluzione di queste dinamiche per poterne avere la certezza. L'assestamento del mercato potrebbe avvenire in primo luogo sul piano nazionale e, in un secondo momento, europeo. Potrebbe verificarsi, infatti, la circostanza in cui – vista la potenziale cessazione del proprio fornitore – gli utilizzatori di tali servizi, abituati ai propri *provider* "locali", potrebbero dapprima migrare verso *competitors* nazionali, per poi considerare, date le aperture di eIDAS 2.0, di rivolgersi a soggetti attivi in altro Paese UE.

Questo pone in una posizione di vantaggio i *provider* attivi negli Stati in cui il legislatore ha nel tempo cercato di inserire, tra i propri requisiti, gli standard internazionali ed europei già ampiamente riconosciuti e diffusi in materia.

Il profilo di conservazione implementativo utilizzato in Italia rappresenta senz'altro una *best practice* nel panorama della *digital preservation* a livello internazionale e, con le opportune contestualizzazioni, potrebbe essere un modello di riferimento per i gruppi di lavoro attualmente impegnati nella definizione degli standard tecnici ed archivistici da utilizzare come riferimento per i nuovi servizi di *electronic archiving* contenuti in eIDAS 2.

In questo senso, il profilo italiano avrebbe tutte le potenzialità per poter costituire una declinazione applicativa da cui partire: i conservatori qualificati sono già conformi agli schemi ISO OAIS, ETSI 119 511 e ISO 16363:2012 *Space data and information transfer systems - Audit and certification of trustworthy digital repositories*, che costituiscono modelli già largamente e universalmente adottati.

Si rende necessario, in ogni caso, valutare con attenzione le evoluzioni del dibattito che nascerà a seguito della definizione dei riferimenti implementativi, in quanto, se il profilo di conservazione che andrà a delinearsi nel perimetro eIDAS 2.0 dovesse discostarsi da quello impiegato in Italia, l'adeguamento dei nostri fornitori al nuovo contesto potrebbe richiedere notevole impegno.

Se è vero, infatti, che quanto agli standard funzionali, di processo e organizzativi l'Italia dovrebbe partire con un certo vantaggio, lo stesso non può dirsi per aspetti più specifici.

La problematica principale da indagare è, infatti, l'interoperabilità. Quanto ai metadati di conservazione, in primo luogo, i conservatori si riferiscono al modello esclusivamente nazionale dell'allegato 5 *I metadati* alle Linee Guida AgID, la cui formulazione è fortemente condizionata dal contesto amministrativo e burocratico della Pubblica Amministrazione italiana e dall'ambito della gestione dei documenti fiscali. Tale corredo potrebbe essere sostituito o incorporato da un nuovo schema di metadatazione volto all'impiego su base europea dei servizi di *electronic archiving*.

Ad esempio, i riferimenti per progetti di portata internazionale come E-ARK[44] e ARCHIVER[45] sono METS - *Metadata Encoding and Transmission Standard* e PREMIS - *PREservation Metadata: Implementation Strategies*, i quali potrebbero rappresentare dei validi candidati per il modello tecnico eventualmente eletto dalla Commissione Europea, ma risultano ad oggi estranei al contesto applicativo italiano (sebbene presenti tra gli standard elencati nell'Allegato 4 *Standard e Specifiche tecniche* alle Linee Guida AgID).

Fondamentale sarà anche la modalità con cui i singoli *provider* dovranno validare la prova dell'avvenuta conservazione prodotta dai rispettivi sistemi al fine di garantire la presunzione di integrità dei dati dal momento della conservazione al recupero dell'oggetto digitale. Anche UNI SInCRO potrebbe risultare non del tutto aderente a questa esigenza: sebbene la presenza di un certificato qualificato apposto sull'evidenza risulti in linea con quanto indicato nel nuovo eIDAS[46], il contenuto dello schema potrebbe non essere del tutto coincidente con quanto verrà stabilito. In questo senso, anche la garanzia della prova dell'avvenuto recupero dell'oggetto tramite il DIP dovrebbe essere rivista, con l'obiettivo finale di disporre di uno strumento di validazione certa, che sia effettivamente in grado di assicurare l'accuratezza e l'interoperabilità delle evidenze di conservazione, e di conseguenza, dei DIP tra i vari *archiving services*.

Occorrerà tuttavia attendere l'esito dei tavoli di lavoro attualmente in corso per avere contezza di quali standard tecnologici e di processo costituiranno la base dei nuovi servizi di archiviazione elettronica qualificata. Si avrà maggiore certezza in proposito entro 12 mesi dall'entrata in vigore del nuovo eIDAS, come da comma 2 dell'articolo 45j:

> 2. By … [12 months from the date of the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Ci si aspetta, come già sostenuto, che le novità importanti non riguarderanno gli aspetti funzionali e organizzativi, che continueranno con ogni probabilità ad essere ancorati a standard *de iure* e *de facto* come OAIS, ISO 16363 e ISO 14641, quanto piuttosto i temi dell'interoperabilità tecnica e delle evidenze di processo.

---

[44] Per approfondimenti sul progetto e-Ark è disponibile la pagina ufficiale <https://www.eark-project.com/> (ultima consultazione 27/03/2024).

[45] Per approfondimenti sul progetto Archiver è disponibile la pagina ufficiale <https://www.archiver-project.eu/> (ultima consultazione 27/03/2024).

[46] Art. 45j, comma 1, lett. d).

Al netto delle considerazioni in merito alle regole tecniche specifiche, eIDAS 2.0 determinerà, per i fornitori di *electronic archiving services* che vogliono caratterizzare il proprio servizio come 'qualificato', l'obbligo di conformarsi ai requisiti generali previsti nel Regolamento per i *Qualified Trust Services Provider*[47].

Questo significherà, anche per gli attuali fornitori, affrontare un nuovo iter di qualificazione presso il competente *supervisory body* che, in contesto italiano, è rappresentato da AgID. Tale circostanza implica, innanzitutto, sottoporre il servizio alle visite ispettive periodiche di un *Conformity Assessment Body*, prassi usuale per i conservatori accreditati prima dell'entrata in vigore del Regolamento per la fornitura AgID (non più necessaria con queste ultime). I *provider* dovranno, inoltre, non solo presentare il *Conformity Assessment Report* all'autorità di vigilanza, ma notificare un avviso a quest'ultima un mese prima dell'audit pianificato, in caso voglia richiedere la partecipazione di un osservatore. Il CAB verificherà non solo gli schemi discendenti dal Regolamento stesso (come l'ETSI 319 401), ma anche la conformità del fornitore a quanto disposto nell'articolo 21 della Direttiva NIS 2, la quale, quindi, diviene parte integrante del sistema di qualificazione a norma eIDAS: oltre alla verifica del report del CAB, AgID dovrà rivolgersi alle autorità competenti di cui alla citata Direttiva, affinché questa svolga attività di vigilanza a tale riguardo e fornisca informazioni sull'esito, al fine di procedere con l'istruttoria. Tale ruolo in Italia sarà riservato all'Agenzia per la Cybersicurezza Nazionale, la quale già attualmente esercita funzioni di controllo sui conservatori che erogano il servizio in modalità cloud e che risultano iscritti nel proprio Marketplace.

Quanto all'esercizio della vigilanza, per l'Italia si prevede che questo continuerà a basarsi sul già esistente *Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. I) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del D Lgs. 7 marzo 2005, n. 82*[48], in ogni caso già richiamato dal *Regolamento sui criteri per la fornitura dei servizi di conservazione*.

I requisiti, certamente non troppo distanti da quelli già previsti per i conservatori in Italia, includono – dal punto di vista organizzativo – l'impiego di personale competente e qualificato, il mantenimento di risorse finanziarie sufficienti, la condivisione pubblica di termini e condizioni del servizio e la stesura di un piano di cessazione. Dal punto di vista della sicurezza, è prescritto l'utilizzo di sistemi e prodotti affidabili e tecnicamente sicuri, l'accesso a questi ultimi solo da parte di figure autorizzate e una tenuta dei dati tale da garantirne l'autenticità. In termini di valutazione del rischio, sarà necessaria la predisposizione di politiche adeguate e l'adozione di misure corrispondenti per gestire i rischi legali, commerciali, operativi e altri rischi diretti o indiretti. Infine, saranno obbligatorie la notifica di incidenti o violazioni alle autorità competenti e la conservazione – anche post cessazione – di

[47] Nello specifico, si tratta dei requisiti fissati agli articoli 21 e 24 del Regolamento eIDAS 2.0.

[48] Il Regolamento, aggiornato al 02/11/2022 è pubblicamente disponibile al link <https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/22305820140O__ORegolamento+vigilanza+14bis+cad.pdf> (ultima consultazione 21/03/2024).

tutte le informazioni pertinenti relative ai dati emessi e ricevuti dal prestatore di servizi fiduciari qualificato.

Si propone, in chiusura, una breve riflessione sul tema degli *archiving services* nel contesto più ampio dell'archivistica e della conservazione dei documenti a cui è stato riconosciuto il valore di beni culturali.

Il Regolamento eIDAS 2.0, per sua stessa prerogativa, non si riserva imposizioni su questo campo di applicazione, come esplicitato dal Considerando 67:

The activities of national archives and memory institutions, in their capacity as organisations dedicated to preserving the documentary heritage in the public interest, are usually regulated in national law and they do not necessarily provide trust services within the meaning of this Regulation. In so far such institutions do not provide such trust services, this Regulation is without prejudice to their operation.

Tuttavia, le nuove prospettive offerte da eIDAS 2.0 con l'introduzione dei *qualified archiving service* e la conseguente e inevitabile revisione del quadro giuridico in vigore in Italia a proposito di conservazione digitale, possono rappresentare lo spunto o lo stimolo che consenta al legislatore italiano di armonizzare il proprio assetto normativo al fine di conciliare i necessari adeguamenti in materia di transizione digitale con i principi di salvaguardia del patrimonio archivistico e culturale, che paiono, attualmente, percorrere dei binari paralleli.

A tal proposito, si renderà necessaria anche una maggiore definizione dell'apparato terminologico: in Italia si stanno realizzando applicativamente delle soluzioni che tengono conto della distinzione tra sistemi conservativi intermedi e permanenti, come il Polo di Conservazione Digitale dell'Archivio Centrale dello Stato[49], ma tale 'separazione' non trova la sua formulazione teorica in alcun provvedimento normativo, sia esso riguardante l'archivistica o la digitalizzazione. Risultano assenti, allo stesso modo, riferimenti che collochino e traspongano le tradizionali definizioni di archivio corrente, di deposito e storico nel contesto digitale, conferendogli uno specifico perimetro rispetto alle corrispondenti soluzioni informatiche sviluppate. La prassi, inoltre, vede il termine 'archiviazione' identificare la fase di gestione documentale, mentre riserva al termine 'conservazione' l'accezione di preservazione a lungo termine dei documenti: con eIDAS 2.0 tale paradigma non risulterà più coerente, in quanto – di fatto – la denominazione unificata per la conservazione digitale a livello europeo sarà quella di *electronic archiving*, dunque archiviazione elettronica.

[49] Per approfondimenti sul progetto è disponibile la pagina ufficiale <https://acs.cultura.gov.it/piano-nazionale-di-ripresa-e-resilienza-del-ministero-della-cultura/polo-di-conservazione-digitale/> (ultima consultazione 27/03/2024).

N. 4 - 2024 - pp. 164-175

Registri elettronici qualificati: tecnologie ed opportunità

Davide Coletto - Giulio Di Clemente

Abstract [IT]: Il tema Registri elettronici impone la fondamentale introduzione dei concetti di blockchain e DLT, ovvero le tecnologie che stanno alla base delle crypto valute. Il presente articolo propone, in primo luogo, l'analisi dei vari tipi di blockchain, approfondendo la distinzione tra, le blockchain pubbliche, private e i consorzi, evidenziando come ciascuna modalità possieda caratteristiche distintive in termini di accessibilità.

In secondo luogo, il contributo avanza nella riflessione sui modelli di consenso, cuore pulsante della blockchain, che garantiscono l'integrità e la fiducia in un ambiente decentralizzato: si esaminano i vari algoritmi di consenso, come Proof of Work (PoW), Proof of Stake (PoS), e Delegated Proof of Stake (DPoS), discutendo le loro peculiarità, i benefici e le complessità.

In conclusione, si presentano una panoramica e una valutazione critica sulla tecnologia blockchain, delineando il suo potenziale impatto sui processi attuali e le sfide future, con un focus particolare sulle implicazioni per i Trust Service Provider nel contesto dei registri elettronici.

Abstract [EN]: The topic of electronic ledgers requires the fundamental introduction of the concepts of blockchain and DLT, i.e. the technologies behind cryptocurrencies. This paper proposes, firstly, an analysis of the various types of blockchain, delving into the distinction between, public, private and consortia blockchains, highlighting how each mode possesses distinctive characteristics in terms of accessibility.

Secondly, the contribution advances in its consideration of consensus models, the beating heart of the blockchain, which guarantee integrity and trust in a decentralised environment: the various consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) are examined, discussing their peculiarities, benefits and complexities.

In conclusion, an overview and critical assessment of blockchain technology is presented, outlining its potential impact on current processes and future challenges, with a particular focus on the implications for Trust Service Providers in the context of electronic ledgers.

Parole chiave: Introduzione alla blockchain, DLT, modelli di consenso, Regolamento 2024/1183 (eIDAS v2), TSP, ruolo dei TSP, Registri elettronici qualificati.

Sommario: 1) Introduzione alle blockchain e standardizzazione attuale. 2) Modelli di Consenso. 3) I Registri Elettronici Qualificati visti dal (futuro) Regolamento eIDAS v2. 4) Ruoli dei TSP e degli operatori dei nodi

Introduzione alle blockchain e standardizzazione attuale

Negli ultimi anni si è sentito parlare molto della tecnologia blockchain, soprattutto nel mondo delle valute digitali, ambito nel quale il loro utilizzo è fondamentale: infatti esse consentono di memorizzare le transazioni in un registro condiviso, garantendo che queste siano sostanzialmente immutabili e decentralizzate.

Diversi enti che si occupano di produrre standard a livello sia europeo sia internazionale, come ETSI, ISO, o ITU, hanno condotto vari studi in ambito blockchain e, più in generale, sulla tecnologia a registro distribuito, o DLT (dall'acronimo inglese Distributed Ledger Technology), per cercare una definizione generalmente condivisa. Seguono alcuni esempi di rilievo (in ordine alfabetico):

- Secondo ILNAS[1], una blockchain può essere vista come un "*registro digitale distribuito e condiviso che registra tutte le transazioni che avvengono in una rete aziendale*". Dire che il registro elettronico è distribuito significa dire che la struttura del database della blockchain è replicata tra molti partecipanti (detti anche "nodi") della rete, ognuno dei quali collabora alla sua manutenzione. Questo porta chiaramente ad un problema di sincronizzazione tra le copie del registro, cioè che tutte le repliche del registro siano uguali tra loro; per far ciò, una rete blockchain utilizza opportuni *meccanismi di consenso*, meglio analizzati in seguito;
- Secondo lo standard ISO 22739:2023 dal titolo "*Blockchain and distributed ledger technologies*", una blockchain si può definire come un "*distributed ledger with confirmed blocks organized in an append-only, sequential chain using hash links*", vale a dire: un registro distribuito con blocchi soggetti a conferma, organizzati in una catena sequenziale in cui l'unica possibile operazione è l'aggiunta di un nuovo blocco, realizzata utilizzando algoritmi crittografici di hash per generare i collegamenti tra un blocco ed il successivo;
- In ITU-T X.1400 si definisce più in generale un registro elettronico come un "*archivio di informazioni che conserva registrazioni finali e definitive (immutabili) delle transazioni*". Quindi, secondo questo standard, un generale registro elettronico ha insito il concetto di immutabilità;

[1] Si tratta dell'istituto lussemburghese di standardizzazione (l'acronimo sta per "Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services").

quest'ultima è definita da ISO come la "*proprietà di un registro elettronico in cui i record del registro stesso non possono essere modificati o rimossi una volta aggiunti*".

Nelle definizioni sopra riportate emergono alcuni concetti rilevanti, come:
- le transazioni;
- i blocchi;
- i collegamenti tra i blocchi mediante funzioni di hash;
- l'immutabilità dei blocchi dopo la loro inclusione nel registro.

Di seguito si dettagliano i primi tre concetti, da cui discende l'ultimo.
- Con il termine "**transazioni**" si intendono le registrazioni di eventi, come lo scambio di risorse tra soggetti o la creazione di nuove risorse; per "risorse" qui si intende qualsiasi bene, rappresentato digitalmente, che possa essere trasferito;
- I **blocchi** sono entità composte da:
- una collezione di transazioni;
- una intestazione di blocco (detta anche "block header");
- I blocchi sono **collegati tra loro tramite un meccanismo crittografico** (generalmente una funzione di hash); il collegamento è generalmente "in avanti", cioè il blocco più giovane nella catena contiene un riferimento al blocco che immediatamente lo precede.

Nelle definizioni di ISO si parla di registri distribuiti; un registro (o anche "registro elettronico") è definito come un "*archivio di informazioni che conserva registrazioni di transazioni destinate a essere finali, definitive e immutabili*". Un registro si dice "*distribuito*" quando esso è "*condiviso, replicato e sincronizzato in modo distribuito e decentralizzato*". I **nodi** sono le entità tra le quali il registro è condiviso e possono essere distinti in due categorie, nel senso che un nodo può essere:
- un **Full-Node**, che mantiene una copia completa del registro distribuito, trasmettendo i dati agli altri nodi; i full-node leggono/scrivono le transazioni e assemblano i blocchi, assicurando che i nuovi blocchi aggiunti siano validi;
- un **Light-Node**, che contiene solo un elenco parziale di transazioni e quindi deve essere collegato ad un full-node per garantire che i dati in esso contenuti siano accurati e utili.

I registri possono essere classificati in diverse tipologie di rete:
- **Rete centralizzata**: è una rete in cui i partecipanti devono comunicare con un'autorità centrale per poter "parlare" tra loro. La topologia della rete è quindi del tipo "a stella"; il problema principale di questo tipo di reti è che in caso di malfunzionamento o distruzione del nodo centrale, l'intera rete smette di funzionare;

- **Rete distribuita**: è una rete in cui ogni partecipante può comunicare con (alcuni degli) altri senza passare attraverso un nodo centrale. Poiché esistono più vie di comunicazione, la distruzione di un singolo nodo non impedisce la comunicazione tra i rimanenti. Questo tipo di rete è nota anche come rete "peer-to-peer";
- **Rete decentralizzata**: è una rete in cui esistono più autorità che fungono da hub per una sottosezione di partecipanti. Poiché alcuni partecipanti si trovano "sotto" un hub centralizzato, la distruzione di quest'ultimo impedirà a tali partecipanti di comunicare, ma i restanti nodi, quelli che si trovano "sotto" altri hub, non risultano affetti da tale evenienza.

Le blockchain, viste come specifici registri distribuiti, si possono classificare in due categorie (almeno per quanto riguarda le politiche di accesso al sistema), vale a dire *permissionless* e *permissioned*, descritte come segue:

- **Blockchain permissionless**: queste sono piattaforme decentralizzate aperte a chiunque, nel senso che chiunque ha la possibilità di pubblicare nuovi blocchi (previo raggiungimento di un qualche tipo di consenso all'interno della rete dei nodi), senza bisogno di autorizzazioni da parte di alcuna autorità comunemente riconosciuta;
- **Blockchain permissioned**: sono quelle in cui gli utenti che pubblicano i blocchi devono essere autorizzati da qualche autorità (sia essa centralizzata o decentralizzata).

Modelli di Consenso

Secondo ISO, il "*consenso*" all'interno di un DLT, è un:
"*accordo tra i nodi DLT sul fatto che:*

1. *una transazione è convalidata;*
2. *che il registro elettronico distribuito contiene un insieme e un ordine coerente di transazioni convalidate*".

Si noti che il raggiungimento del consenso non implica necessariamente che tutti i nodi DLT siano d'accordo sullo stato del registro elettronico.

Un "meccanismo di consenso" (o "modello di consenso") è quindi semplicemente un "insieme di regole e procedure con cui si raggiunge il consenso".

Il NIST statunitense, con il rapporto IR 8202, tratta in modo approfondito degli algoritmi di consenso. Viene giustamente evidenziata una differenza tra i modelli di consenso delle blockchain permissionless e quelli delle blockchain permissioned, ovvero il fatto che, mentre nelle permissioned può esistere un certo livello di fiducia tra i nodi, in quelle permissionless gli utenti non si fidano l'uno dell'altro, rendendo così il modello di consenso un punto altamente critico nell'architettura del sistema.

Il NIST analizza diversi algoritmi di consenso, tra cui:

- Prova di lavoro (o **PoW**, dall'inglese Proof of Work);
- Prova di puntata (o **PoS**, dall'inglese Proof of Stake);
- Prova di autorità/prova di identità (o **PoA**, dall'inglese Proof of Authority);
- Prova del tempo trascorso (o **PoET**, dall'inglese Proof of Elapsed Time);
- Round Robin.

Di seguito vengono analizzati quelli ritenuti più rilevanti, vale a dire PoW, PoS e PoA.

PoW

Il NIST afferma che, nel modello proof of work, un utente pubblica un nuovo blocco quando si trova ad essere il primo a risolvere un problema computazionalmente complesso, il che costituisce la prova che l'utente ha svolto un certo lavoro. Uno dei problemi comunemente utilizzati è richiedere che l'hash (dell'intestazione) di un blocco sia inferiore a un certo valore, il che significa che l'hash in questione, che è di lunghezza predeterminata e fissata, deve iniziare con un certo numero di zeri. La scelta di quanti debbano essere gli zeri iniziali dipende dalla difficoltà che si desidera che il problema abbia; tale difficoltà è calibrata per mantenere approssimativamente costante il tasso di creazione dei nuovi blocchi e, stante la natura crittografica delle funzioni di hash, la difficoltà non varia dopo aver risolto molti problemi, in quanto due problemi diversi sono indipendenti, e l'unica strategia di risoluzione possibile è quella di effettuare tentativi ripetuti (quindi un metodo a *forza-bruta*). È questo, ad esempio, il meccanismo utilizzato nella blockchain di Bitcoin e, fino al 2022, anche da Ethereum.

PoS

Il NIST afferma che il modello proof of stake (PoS) si basa sull'idea che più risorse un utente ha investito nel sistema, più è probabile che voglia che il sistema abbia successo e meno è probabile che voglia sovvertirlo.

L'idea è quindi che gli utenti investano la propria ricchezza, ad esempio in termini di criptovaluta, o comunque una risorsa scarsa, nel sistema; la quantità di tali risorse a disposizione di un utente determina la capacità di pubblicare nuovi blocchi. La PoS differisce molto dalla PoW, tra l'altro, anche per quanto riguarda i consumi energetici: mentre la PoW è piuttosto energivora, la PoS non consuma elevate quantità di elettricità o di potenza di calcolo. È questo il meccanismo usato, a partire dal 2022, da Ethereum.

PoA

Al contrario dei precedenti modelli di consenso, nella Proof of Authority si

prevede che ci sia un certo livello di fiducia tra i nodi, che devono essere legati a un'identità del mondo reale; infatti, i nodi validatori devono confermare le proprie identità reali, registrandole sulla blockchain. Questo modello di consenso ha senso solo all'interno di blockchain permissioned, in quanto c'è bisogno di una verifica, da parte di una qualche autorità di registrazione, dell'identità presunta degli utenti. L'idea di fondo in questo modello è che i nodi validatori stiano effettivamente mettendo in gioco la loro identità, e quindi anche la loro reputazione, per poter aggiungere nuovi blocchi, così che quando la reputazione di un utente decresce, sarà meno probabile che esso possa pubblicare nuovi blocchi; è quindi compito di ciascun utente della rete mantenere una reputazione elevata, garantendo così, come effetto "collaterale", il corretto funzionamento della stessa. È questo il meccanismo usato, per esempio, in Hyperledger Fabric e anche in EBSI.

I Registri Elettronici Qualificati visti dal (futuro) Regolamento eIDAS v2

Analisi normativa

Finora si è parlato di "blockchain" o di "DLT" e, più in generale, di registri distribuiti, ma questa terminologia non è quella scelta a livello europeo nell'ambito della Revisione del Regolamento eIDAS (o anche eIDAS 2): in quest'ultimo ambito si preferisce parlare, più generalmente, di "registri elettronici", senza mettere in evidenza una particolare struttura della sequenza dei blocchi di dati (come evocato dal termine "blockchain") né una particolare topologia della rete dei nodi (come invece insito nel termine "DLT", la cui lettera "D" sta per "Distributed", cioè distribuito).

Al contrario dell'originario Regolamento eIDAS del 2014, la sua Revisione (Marzo 2024) introduce a livello normativo una distinzione tra *registri elettronici* e *registri elettronici qualificati*, trattati rispettivamente dall'art. 45 duodecies e dall'art. 45 terdecies. Alcune considerazioni generali si trovano anche nel Considerando 68; nei paragrafi seguenti viene effettuata una disamina di tutte queste parti del Regolamento.

Creazione e gestione di un registro elettronico qualificato

L'articolo 45 terdecies, paragrafo 1, lettera a), in eIDAS 2 afferma che i registri elettronici qualificati:

"sono creati e gestiti da uno o più prestatori di servizi fiduciari qualificati".

Il significato preciso di "creato" e di "gestito" va esplicitato, in quanto non risulta lampante a prima vista.

L'interpretazione fornita qui è che:

- la creazione del registro elettronico qualificato richiede che il primo blocco del registro elettronico, detto anche "blocco genesi", deve essere creato da un QTSP e, facoltativamente, da uno o più ulteriori TSP o QTSP[2];
- la gestione del registro elettronico qualificato prevede che i nodi che partecipano alla costruzione del registro elettronico debbano essere riconosciuti dal QTSP "creatore" (o dai QTSP creatori, se più di uno), ad esempio mediante identificazione da parte di quest'ultimo, nonché avere un qualche tipo di relazione legale, organizzativa e tecnica con il/i QTSP responsabile/i del sistema. È utile precisare che, come meglio discusso nel seguito, gli operatori dei nodi non devono necessariamente essere dei QTSP o dei TSP.

Seguono alcune considerazioni legate al rapporto col GDPR: se i nodi che gestiscono l'infrastruttura fanno parte di un gruppo ben definito, la partecipazione a questo gruppo richiede la definizione di tutte le responsabilità legali nella gestione dell'infrastruttura, compresa la definizione di:

- chi è il titolare del trattamento dei dati;
- chi è il responsabile del trattamento dei dati.

Come conseguenza, i contratti che definiscono la partecipazione a uno specifico registro elettronico qualificato devono coprire questo aspetto e chiarire i doveri dei partecipanti, compresi gli operatori dei nodi.

Si osserva che il richiedere che tutti i nodi siano identificati a priori contrasta un possibile attacco ad alcuni protocolli di consenso, ovvero l'**attacco Sybil**, che consiste nel fatto che un nodo produca molte repliche di se stesso, creando così nodi fittizi, ognuno dei quali viene aggiunto all'insieme dei nodi; in questo modo, potrebbe controllare la rete, avendo a disposizione la maggior parte dei nodi.

Nel caso in cui ai nodi venga data un'identità da uno o più QTSP, è impossibile per un nodo malintenzionato produrre queste repliche, portando all'inapplicabilità dell'attacco. Ciò ha un'implicazione più profonda per il protocollo di consenso utilizzato dai nodi dell'infrastruttura. Il Regolamento, in effetti, non parla di consenso, ma è opportuno che vengano fatte alcune considerazioni in merito, soprattutto riguardo alle sue funzionalità, nel senso che un meccanismo di consenso dovrebbe:

- Essere basato su un principio di maggioranza, nel senso che sicuramente, se una quota pari al 50% + 1 dei nodi hanno raggiunto un accordo su un nuovo blocco, questo dovrebbe essere considerato sufficiente per considerare che c'è accordo sul nuovo blocco da inserire. C'è da considerare, però, che nodi

[2] Un TSP è un Trust Service Provider, ovvero un prestatore di servizi fiduciari; questi sono alcuni specifici servizi elettronici, normalmente forniti dietro pagamento di un compenso, elencati nel Regolamento eIDAS (già nella versione originaria del 2014); ad esempio, rientrano tra i servizi fiduciari la creazione e la verifica di firme e sigilli elettronici. Un QTSP è un particolare TSP che ha sostenuto con successo un processo di accreditamento presso un organismo di supervisione; i QTSP sono soggetti a vincoli giuridici più stringenti dei "normali" TSP.

diversi potrebbero avere un "peso", inteso come potere di voto, diverso l'uno dall'altro, e la soglia di maggioranza quindi potrebbe essere più alta di quanto qui ipotizzato;

- Essere deterministico: a parità di input, cioè dato uno specifico stato del registro e dei nodi, l'output, inteso come identità del successivo blocco aggiunto, deve essere univoco;
- Dovrebbe essere definitivo: una volta che una transazione (o meglio, un blocco) è finalizzato, non può più essere rimosso dal sistema.

Affidabilità dei dati nel registro

L'articolo 45 terdecies, paragrafo 1, lettera b) , in eIDAS 2 stabilisce che i registri elettronici qualificati:

"stabiliscono l'origine delle registrazioni di dati nel registro".

La più diretta interpretazione di questo requisito è che i QTSP che gestiscono il registro elettronico devono essere a conoscenza dell'identità dei nodi che aggiungono blocchi al registro elettronico stesso, in accordo con l'interpretazione data del requisito precedente, secondo cui i nodi che partecipano al registro elettronico devono essere identificati dai QTSP creatori. Un'interpretazione un po' più approfondita di questo comma ruota attorno alla provenienza dei dati memorizzati nel registro elettronico stesso: potrebbe non essere sufficiente sapere che questi dati sono stati memorizzati nel registro elettronico da un certo nodo, ma sarebbe necessario sapere anche la fonte originaria di questi dati. È presumibile che una determinazione precisa su questo punto verrà presa anche nell'ambito del Data Act.

Ordinamento temporale

L'articolo 45 terdecies, paragrafo 1, lettera c), in eIDAS 2 stabilisce, con riferimento ai registri elettronici qualificati, che:

"garantiscono l'ordine cronologico sequenziale univoco delle registrazioni di dati nel registro".

Questo requisito sancisce che i registri elettronici sono strutture dati lineari nel tempo. In realtà, garantire l'ordine cronologico può essere una sfida impegnativa, in quanto le transazioni che vengono generalmente raggruppate in blocchi, ma le transazioni inserite nello stesso blocco non possono essere confrontate da un punto di vista cronologico, a causa della natura distribuita e quindi asincrona del registro; è però corretto che blocchi diversi siano effettivamente suscettibili di ordinamento, nel senso che, dati due blocchi, si vorrebbe sapere quale dei due è stato aggiunto per primo al registro.

Questo requisito potrebbe essere soddisfatto a livello di blocco, con un timestamp applicato all'intero blocco, oppure a livello di transazione, anche ad opera di

chi crea la transazione, con un timestamp specifico.

Inoltre, si sottolinea che il Considerando 68 contiene un punto specifico rilevante per la struttura di un registro elettronico (qualificato), in quanto afferma che tali registri sono una sequenza di record di dati. Pertanto, si dovrebbe considerare questo come l'unico aspetto strutturale di un registro (qualificato) previsto dal nuovo Regolamento, e limitarsi ad un ordinamento tra blocchi diversi, piuttosto che tra transazioni nello stesso blocco.

Rilevamento di tentativi di alterazione e integrità nel tempo

L'articolo 45 terdecies, paragrafo 1, lettera d) , in eIDAS 2 stabilisce, riguardo ai registri elettronici qualificati, che:

"registrano i dati in modo tale che sia possibile individuare immediatamente qualsiasi successiva modifica degli stessi, garantendo l'integrità nel tempo".

Sostanzialmente, quindi, una volta che i blocchi sono stati accettati nella catena, qualsiasi modifica ad essi apportata deve essere rilevabile, garantendo così la sicurezza del registro. Tale compito di vigilanza dovrebbe spettare unicamente al QTSP responsabile del sistema. Generalmente questa verifica di sicurezza è implementata per via di un legame crittografico tra un blocco e il suo successore, ad esempio sotto forma di funzione di hash: ogni blocco (tranne il blocco genesi) potrà ad esempio contenere al suo interno un hash del blocco precedente, in modo da rendere evidente tentativi di modifica di un blocco nel passato: infatti, se venisse sostituito un blocco "nel mezzo" della catena, si verrebbe ad alterare il suo hash (in base alle proprietà[3] delle funzioni di hash), rendendo evidente la tentata manomissione.

Ruoli dei TSP e degli operatori dei nodi

È opportuno notare che, in eIDAS 2, i registri elettronici rappresentano una nuova categoria di servizi fiduciari; infatti, erano del tutto assenti nel Regolamento eIDAS originario (2014).

---

[3] Le funzioni di hash devono soddisfare alcuni requisiti, vale a dire:
- l'essere deterministiche (fissata la funzione di hash e fissato l'input, l'output è sempre lo stesso) e avere inoltre lunghezza fissa (la lunghezza dell'output, indipendentemente da quella dell'input, è sempre la stessa);
- l'essere difficili da invertire (dato l'hash di un dato, deve essere computazionalmente difficile ricostruire quel dato se ne è noto solo l'hash);
- godere dell'effetto valanga (cambiando anche un solo bit dell'input, l'output deve risultare completamente diverso;
- Il calcolo di un hash di un dato dovrebbe essere computazionalmente semplice.

In questo paragrafo ci si concentra su:
- i requisiti di sicurezza che un fornitore di tale servizio deve soddisfare;
- i ruoli ricoperti dai gestori dei nodi in un Registro elettronico.

Come analizzato in precedenza, un registro elettronico qualificato è gestito da uno o più TSP, mentre (la fornitura di) un registro non qualificato è comunque un servizio fiduciario, che quindi deve essere realizzata da un TSP, che non è necessariamente qualificato, ma è comunque soggetto ad una serie di vincoli tecnici e organizzativi e, in tutti i casi, alla Direttiva NIS2. Nel caso dei registri qualificati, i QTSP che li gestiscono hanno alcuni obblighi aggiuntivi espressi principalmente dall'art. 45l: infatti, la fornitura di un registro elettronico qualificato richiede di soddisfare alcuni vincoli sui ruoli ricopribili dagli attori in gioco; tali ruoli possono essere impersonati dai QTSP, dai TSP o in generale da qualsiasi organizzazione adatta, come indicato di seguito. I ruoli degli operatori dei nodi all'interno dei registri elettronici sono sostanzialmente quattro, a seconda che il registro centralizzato o decentralizzato, qualificato o non qualificato.

Caso 1: registri elettronici qualificati decentralizzati

In questo primo caso, i nodi potrebbero essere classificati in:

Gestori

Il QTSP che istanzia un registro elettronico qualificato si potrebbe denominare "**gestore**", in quanto dà l'avvio alla creazione del sistema, ma poi si occupa anche della relativa gestione, avendo in capo svariate questioni tecnico-operative, tra cui:

a) aggiunta/rimozione di nodi al/dal sistema;
b) formulazione dei quadri tecnici e legali con una relativa suddivisione delle responsabilità;
c) Sviluppo e manutenzione dell'architettura tecnica del sistema.

Costruttori

I blocchi successivi al primo possono essere "costruiti" da nodi (delegati ad hoc o semplicemente interessati ad aggiungere nuove informazioni al registro) che essenzialmente eseguono l'algoritmo di consenso; un nodo siffatto, detto "costruttore", deve essere gestito da un QTSP in quanto fornisce una funzione fondamentale del sistema, direttamente collegata alle sue caratteristiche di sicurezza.

Validatori

I blocchi appena creati devono essere convalidati, sia sintatticamente sia semanticamente, per quanto riguarda il loro contenuto in termini di singole transazioni memorizzate. I nodi deputati a ciò possono essere chiamati "validatori" e possono

essere gestiti previo accordo specifico con il QTSP responsabile del registro.

Replicatori

Alcuni nodi potrebbero non essere interessati né alla costruzione né alla convalida di nuovi blocchi, ma semplicemente a ospitare una copia del registro elettronico a beneficio degli altri utenti, venendo per questo ricompensati; nodi siffatti potrebbero essere chiamati "replicatori", poiché l'unica loro azione è quella di "inoltrare" dati ad altri utenti; chiunque, previo accordo con il QTSP che gestisce il registro elettronico qualificato, potrebbe divenire un replicatore.

Il successo delle PKI nel garantire che, ad esempio su Internet, persone diverse possano parlarsi senza prima conoscersi, con ragionevole fiducia del fatto che i destinatari dei propri messaggi siano corretti, spinge a considerare quello delle PKI come un modello da replicare; ecco perché si ritiene che si possa adottare un analogo modello nell'ambito dei registri elettronici qualificati. Si può pensare quindi che ci siano dei nodi (e degli operatori) responsabili del generale buon andamento del sistema e della sua conformità legale. Altri nodi potranno svolgere le funzioni più propriamente tecniche, come ad esempio la validazione; infine, nel caso di sistemi ad alte prestazioni con un numero di utenti elevato, alcuni nodi potranno essere dedicati a svolgere la funzione di repliche (in lettura).

Caso 2: registri elettronici qualificati centralizzati:

Nel caso in cui il registro elettronico sia un sistema centralizzato, uno dei QTSP che partecipa al sistema potrebbe impersonare tutti i diversi ruoli summenzionati, dove i ruoli di gestore e costruttore possono essere svolti dalla stessa organizzazione, mentre i validatori e i replicatori potrebbero essere forniti internamente o esternalizzati.

Tutti questi soggetti hanno rapporti giuridici tra loro e sono soggetti a obblighi legali. Ad esempio, tutte le identità di questi soggetti devono essere riconosciute dal gestore (o dai gestori); i costruttori di consenso possono avere rapporti commerciali o giuridici tra loro e/o con il gestore (o i gestori). Per quanto riguarda i mirrors, essi devono rispettare alcuni requisiti di sicurezza per non permettere a chiunque di leggere o scrivere sul registro elettronico.

Casi 3 e 4: registri elettronici non-qualificati centralizzati o decentralizzati:

Per i registri elettronici non qualificati, invece, il quadro si semplifica, grazie alla minor quantità di vincoli giuridici. La struttura discussa al Caso 1 potrebbe ancora essere funzionalmente applicata, poiché un generale registro elettronico potrebbe essere implementato in molti modi diversi e dovrebbe essere il fornitore a definire

l'architettura più adatta. In sostanza, ci si limita ad avere uno o più TSP nel ruolo di gestore, mentre gli altri nodi del sistema potrebbero essere forniti da TSP o da organizzazioni idonee, mentre i costruttori potrebbero essere implementati da nodi gestiti dai TSP o anche altra organizzazione.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 176-185

Il nuovo sistema sanzionatorio in eIDAS 2.0: ruolo di AgID e questioni applicative

Massimiliano Nicotra

Abstract: L'articolo esamina le modifiche apportate al Regolamento eIDAS, con particolare attenzione alle nuove disposizioni sanzionatorie introdotte. Dopo un'analisi dettagliata del nuovo art. 16 del Regolamento si evidenziano le differenze e similitudini con alcuni meccanismi sanzionatori introdotti da altre norme regolamentari europee, nonché i principi di proporzionalità, effettività e dissuasività previsti per regolare l'applicazione delle sanzioni da parte degli Stati membri, ciò affinché esse riflettano la gravità della violazione e il contesto economico del trasgressore.

Ci si sofferma nell'analisi dell'attuale sistema sanzionatorio, come regolato dall'art. 32 bis del CAD e dal Regolamento interno di AgID, evidenziando alcune antinomie interne dello stesso anche alla luce dei principi dettati dalla giurisprudenza europea e costituzionale.

Dal confronto tra la nuova disciplina europea e quella attualmente vigente in Italia emerge che sarà necessaria una maggiore specificazione delle condotte volative delle norme regolamentari ed interne, nonché l'introduzione di un reale meccanismo di gradazione delle sanzioni pecuniarie, alla luce sia dei principi di regolamentari sia delle disposizioni di diritto interno (L. n. 689/1981) in materia di sanzioni amministrative.

Parole chiave: regolamento eIDAS – sanzioni amministrative – principi di effettività, proporzionalità ed effettività – gradazione – condotte sanzionate – normativa nazionale – autorità di vigilanza

Sommario: 1. Le sanzioni nel Regolamento eIDAS: uno sguardo d'insieme – 2. Ambito soggettivo delle sanzioni – 3. Le condotte sanzionabili – 4. L'attuale sistema sanzionatorio del Codice dell'Amministrazione Digitale – 5. Le questioni applicative del "nuovo" art. 16 alla disciplina di diritto interno

1. Le Sanzioni nel Regolamento eIDAS: uno sguardo di insieme

Tra le modifiche di rilievo apportate al Regolamento n. 910/2014 vi è l'introduzione, da parte della nuova disciplina, di un sistema sanzionatorio a livello di normativa comunitaria, elemento non previsto nella versione originaria.

Il nuovo art. 16 del Regolamento, infatti, prevede l'obbligo per gli Stati membri di introdurre negli ordinamenti nazionali delle sanzioni per le violazioni di quanto stabilito nel Regolamento stesso, indicato, quali criteri principali per tale adozione, quello della effettività, proporzionalità e dissuasività.

Si tratta di criteri che oramai sono abbastanza comuni nella disciplina europea che regola il settore tecnologico, con un approccio più simile a quello dei regolamenti più recenti (Regolamento (UE) 2022/2065 - Digital Service Act) rispetto a quello contenuto nel Regolamento Generale per la Protezione dei Dati (Regolamento n. 679/2016). Tale ultima normativa non prevede una delega, che in effetti è più confacente allo strumento delle direttive europee, ai singoli Stati per l'adozione di norme di diritto interno in attuazione della previsione europea, ma stabilisce direttamente, sotto il profilo delle sanzioni pecuniarie, i limiti massimi che le autorità di controllo possono applicare in caso di violazione della normativa in materia di protezione dei dati personali, dettagliando le ipotesi di applicazione, con rinvio a specifiche norme del Regolamento stesso, ed indicando dei criteri di gradazione a cui le Autorità stesse debbono attenersi.

La scelta compiuta dal legislatore europeo nella sede in esame è invece diversa: il legislatore nazionale dovrà introdurre nel diritto interno le sanzioni, seguendo i criteri dettati dall'art. 16, individuando così le condotte che possono essere oggetto delle stesse, contemporaneamente dovendo assicurare il rispetto dei principi già menzionati di effettività, dissuasività e proporzionalità.

In relazione a tali principi è possibile precisare che le sanzioni devono tendere al ripristino della conformità alla normativa oppure alla punizione di una condotta antigiuridica, ed è in tal senso che va valutata la effettività delle stesse, intesa quale capacità di condurre a tale risultato nel caso concreto.

Il principio di proporzionalità implica che dette sanzioni devono prevedere dei criteri di gradazione, nel senso di dover condurre ad una valutazione diversa in relazione a condotte diverse, comportando che il legislatore nazionale sarà tenuto a diversificare le previsioni sanzionatorie a seconda della gravità della violazione delle norme regolamentari, non potendo essere prevista un'unica sanzione per differenti condotte.

Strettamente correlato ai due principi sopra menzionati, effettività e proporzionalità, è quello di effettività che evidenzia il carattere preventivo del sistema sanzionatorio: la sanzione deve essere in grado di dissuadere un soggetto dal realizzare la condotta violativa del precetto regolamentare. Ciò significa che il meccanismo di punizione per la violazione deve essere tale da scoraggiare il compimento del com-

portamento a cui viene attribuito disvalore, ciò tenuto conto delle caratteristiche soggettive di coloro a cui è diretta la sanzione stessa.

È in tal e contesto che devono essere lette le previsioni dell'art. 16, 2° comma di recente introduzione, in cui viene stabilito un importo massimo di almeno 5.000.000 di Euro per le persone fisiche e, per le persone giuridiche, in alternativa all'ammontare così stabilito di 5.000.000 di Euro, un importo pari all'1% del fatturato mondiale totale annuo dell'impresa, se superiore.

Sulle modalità di calcolo di tale secondo importo si può tenere conto della pronuncia della Suprema Corte di Cassazione n. 27189 del 22 settembre 2023, la quale, relativamente all'analoga fattispecie sanzionatoria di cui all'art. 84 del Regolamento n. 679/2016 ha avuto modo di precisare che le sanzioni pecuniarie applicate alle imprese, qualora siano superiori a quelle stabilite nel massimo dalla norma non possono eccedere la percentuale di fatturato mondiale complessivo di un'impresa prevista dal Regolamento per dette sanzioni.

L'art. 16 al terzo comma conclude introducendo la possibilità, a seconda dei diversi ordinamenti giuridici degli Stati membri, che l'organismo di vigilanza abbia l'autorità di avviare l'azione sanzionatoria, demandato poi l'irrogazione vera e propria della stessa ad un tribunale nazionale. Tale meccanismo, però, non può andare a discapito dell'efficacia dell'azione sanzionatoria stessa, dovendo garantire un effetto equivalente a quello che si avrebbe in caso di imposizione diretta da parte dell'autorità di controllo.

Infine, è bene evidenziare che la norma fa salva l'applicazione dell'art. 31 della direttiva (UE) 2022/2555. Si tratta delle disposizioni che, nell'ambito di tale direttiva (cd. NIS 2) consentono agli Stati membri di introdurre previsioni per l'esercizio efficace da parte delle proprie autorità di controllo competenti delle funzioni di vigilanza ed esecuzione per assicurare il rispetto dei livelli di cibersicurezza previsti, con margini di discrezionalità da parte degli Stati ben più ampi rispetto a quelli stabiliti nel nuovo Regolamento eIDAS.

2. Ambito soggettivo delle sanzioni

Dal punto di vista soggettivo l'art. 16 prevede che possano essere sanzionati i prestatori di servizi fiduciari qualificati e non qualificati. Tale delimitazione non emerge immediatamente dalla lettura dell'articolo, in quanto il primo comma sembrerebbe consentire agli Stati membri di stabilire le sanzioni applicabili in ogni caso di violazione delle norme regolamentari, e, quindi, anche ad esempio agli utenti dei servizi fiduciari o ad altre terze parti. A chiarire la portata soggettiva, restringendola nel senso sopra indicato, è però la formulazione del secondo comma, in cui nel definire gli importi massimi, anzi nell'indicare l'importo massimo base da cui gli Stati membri devono partire, chiarisce che "*tali violazioni da parte dei prestatori di servizi fiduciari qualificati e non qualificati*" siano soggette alle sanzioni amministrative

pecuniarie di importo massimo di almeno quello indicato nel comma medesimo.

La locuzione "tali violazioni" deve quindi essere riferita alle violazioni specificate al primo comma, in cui è conferito il potere generale degli Stati membri di stabilire le relative sanzioni, così limitando la portata della previsione alla sola possibilità di applicare sanzioni ai prestatori di servizi fiduciari qualificati e non.

La lettura dei Considerando nn. 44 e 45 del nuovo testo regolamentare consente di ulteriormente chiarire il punto. L'art. 16 attua direttamente la previsione del Considerando n. 44[1], mentre l'applicazione di quanto riportato nel Considerando 45 - in cui è previsto che gli Stati membri dovrebbero poter stabilire delle sanzioni anche relativamente alle pratiche che generano confusione tra i servizi fiduciari qualificati e non qualificati, o in caso di uso abusivo del marchio di fiducia UE da parte di prestatori di servizi fiduciari non qualificati - appare essere prevista in via indiretta nella più generale formulazione dell'art. 16 stesso. Ciò comporta che tali fattispecie dovranno essere considerate necessariamente dal legislatore nazionale introducendo, sulla base dell'indicazione generale dell'art. 16, una disposizione specifica nell'ordinamento interno che sanzioni le condotte descritte nel Considerando 45.

L'ampliamento dell'elenco dei servizi fiduciari contenuto nell'art. 3, primo comma, n. 16)[2] comporta anche l'ampliamento dei soggetti a cui è applicabile il nuovo regime sanzionatorio. Secondo il regolamento, infatti, un prestatore di servizi fiduciari è qualsiasi persona fisica o giuridica che presta uno o più servizi fiduciari. La prestazione può essere resa o nella qualifica di prestatore di servizi fiduciari qualificato o non qualificato. Mentre la qualificazione deriva da un'apposita assegnazione di tale riconoscimento da parte dell'organismo di vigilanza – a valle delle procedure e verifiche previste dalla normativa – la semplice prestazione di uno dei servizi indicati dal Regolamento eIDAS quali servizi fiduciari implica l'assunzione

---

[1] Considerando 44: *Al fine di garantire l'efficace applicazione del presente regolamento, è opportuno stabilire un limite minimo per il livello massimo di sanzioni amministrative per i prestatori di servizi fiduciari sia qualificati che non qualificati. Gli Stati membri dovrebbero prevedere sanzioni effettive, proporzionate e dissuasive. Nel determinare le sanzioni è opportuno tenere debitamente conto delle dimensioni dei soggetti interessati, dei loro modelli di business e della gravità delle violazioni.*

[2] Secondo tale previsione è un servizio fiduciario un servizio elettronico prestato normalmente dietro remunerazione consistente in uno qualsiasi dei seguenti: a) il rilascio di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; b) la convalida di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari; c) la creazione di firme elettroniche o sigilli elettronici; d) la convalida di firme elettroniche o sigilli elettronici; e) la conservazione di firme elettroniche, sigilli elettronici, certificati di firme elettroniche o certificati di sigilli elettronici; f) la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza; g) il rilascio di attestati elettronici di attributi; h) la convalida di attestati elettronici di attributi; i) la creazione di validazioni temporali elettroniche; j) la convalida di validazioni temporali elettroniche; k) la prestazione di servizi elettronici di recapito certificato; l) la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove; m) l'archiviazione elettronica di dati elettronici e di documenti elettronici; n) la registrazione di dati elettronici in un registro elettronico.

della qualifica di "prestatore di servizi fiduciari non qualificati" con il conseguente assoggettamento al regime sanzionatorio.

La nuova previsione dell'art. 16, pertanto, dovrà già dal solo punto di vista di applicazione soggettiva delle sanzioni, comportare una modifica dell'art. 32 bis del D.l.vo n. 82/2005 (cd. Codice dell'Amministrazione Digitale), il quale nella sua attuale formulazione conferisce all'Agenzia per l'Italia Digitale un potere sanzionatorio nei soli confronti dei prestatori di servizi fiduciari qualificati, dei gestori di posta elettronica certificata, dei gestori dell'identità digitale e dei conservatori.

3. Le condotte sanzionabili

L'irrogazione delle sanzioni, secondo la nuova previsione dell'art. 16 del Regolamento eIDAS, dovrà essere prevista "*in caso di violazioni del presente regolamento*". È evidente, quindi, che la norma regolamentare non contiene un'espressa indicazione delle condotte che possono comportare l'applicazione di una sanzione, neanche tramite un rinvio agli articoli del Regolamento eIDAS la cui violazione può determinarle, ma sarà compito del legislatore nazionale effettuare tale individuazione.

Sotto tale profilo deve rilevarsi che recentemente, in applicazione dell'analoga previsione contenuta all'art. 52 del Regolamento (UE) 2022/2065 (Digital Service Act)[3] il nostro legislatore nazionale con il Decreto-Legge convertito con modificazioni dalla L. 13 novembre 2023, n. 159, ha introdotto all'art. 1 della L. 31 luglio 1997, n. 249 il comma 32 bis, in cui ha individuato, tramite il rinvio agli articoli contenuti nel medesimo DSA, le condotte passibili di sanzioni amministrative pecuniarie, contestualizzando in tal modo l'ambito oggettivo della generica previsione regolamentare.

Le modalità con cui il legislatore nazionale andrà ad individuare le condotte sottoposte a sanzione amministrativa sulla base del richiamato "nuovo" art. 16 assume rilevanza nel momento in cui si tenga a mente la ricostruzione operata dalla dottrina circa la natura di tale istituto[4], che viene distinto per il suo elemento finalistico di portata eminentemente afflittiva connotandolo in termini sostanzialmente coincidenti alla sanzione penale (e, quindi, differenziandosi dalla natura riparatoria della sanzione civile).

---

[3] Il quale al primo comma recita: "*Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione del presente regolamento da parte dei fornitori di servizi intermediari che rientrano nella loro competenza e adottano tutte le misure necessarie per assicurarne l'applicazione in conformità dell'articolo 51*.".

[4] Senza qui voler ripercorrere i numerosi interventi in merito si segnalano E. CANNADA BARTOLI, *Illecito (diritto amministrativo)*, in *Enc. del diritto*, vol. XX, Milano, 1970; E. CAPACCIOLI, *Principi in tema di sanzioni amministrative: considerazioni introduttive*, in *Le sanzioni in materia tributaria. Atti del Convegno di studio svoltosi a Sanremo, 21-22 ottobre 1978*, Milano, 1979, 125 ss.; M.A. SANDULLI, *La potestà sanzionatoria della pubblica Amministrazione*. Studi Preliminari, Napoli, 1981.

Tale coincidenza è stata rimarcata anche dalla Corte europea dei diritti dell'uomo, che con la decisione 8 giugno 1976, Engel e altri c. Paesi Bassi (cause nn. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72) ha ritenuto applicabile il regime dell'art. 6 CEDU in presenza di una "accusa penale" indipendentemente dalla qualificazione giuridica fornita dall'ordinamento nazionale, ciò anche al fine di evitare che uno Stato, qualificando in maniera diversa una certa condotta come illecito amministrativo (o disciplinare) piuttosto che penale, possa eludere la portata applicativa degli articoli 6 e 7 CEDU. La Corte ha così definito dei parametri, noti come "*Engel criteria*", volti a verificare la natura della sanzione adottata da un ordinamento verso una condotta, includendovi qualsiasi privazione della libertà personale imposta a fini punitivi, la natura delle conseguenze previste dalla norma sanzionatoria – che assumono carattere "penalistico" ove prevedano l'adozione di misure punitive/afflittive e non riparatorie o risarcitorie, nonché la significatività di tali conseguenze. Tali parametri sono alternativi e non cumulativi: in presenza di uno di essi deve concludersi per il carattere penale dell'illecito[5], e sono stati applicati anche in ipotesi di applicazione di sanzioni pecuniarie irrogate da un'Autorità amministrativa indipendente per violazione della normativa a tutela della concorrenza[6].

Le sentenze della Corte di Strasburgo hanno avuto influenza anche sulle pronunce della Corte Costituzionale (si vedano tra le altre Corte cost., 4 giugno 2010, n. 196, Corte Cost. 18 aprile 2014, n. 104) che hanno affrontato il tema dell'applicabilità alle sanzioni amministrative di natura afflittiva dei principi di matrice penale, tra cui quello contenuto all'art. 25, 2° comma della Costituzione.

Il richiamo all'art. 7 CEDU, infatti, pone proprio il problema della necessaria definizione della condotta che l'ordinamento giudica con disvalore ai fini di una possibile punizione della stessa. Ed, infatti, traendo le conclusioni dalla ricostruzione sopra operata, il carattere tipicamente afflittivo e di natura simil-penalistica della sanzione amministrativa dovrebbe far ritenere necessario che il legislatore nazionale individui con un certo grado di determinatezza quali sono le condotte specifiche che possono essere oggetto di sanzione.

Il tema assume rilevanza specifica nella materia che stiamo trattando, dato che, come si vedrà, l'attuale disciplina prevista dall'art. 32 bis, 1° comma, del Decreto

---

[5] Tali criteri sono stati ribaditi in varie decisioni della Corte di Strasburgo, tra cui Corte eur. dir uomo, Grande Camera, 23 novembre 2006, *Jussila c. Finlandia*, (ric. n. 73053/01) § 31; Id., 9 ottobre 2003, *Ezeh e Connors c. Gran Bretagna* (cause nn. 39665/98 e 40086/98) § 120; Id., Sezione Seconda, 27 settembre 2011, *Menarini Diagnostics S.r.l. c. Italia* (ric. n. 43509/08) § 38; Id., Quarta Sezione, 20 maggio 2014, *Nykänen c. Finlandia* (ric. n. 11828/11) § 39.

[6] Sezione Seconda, 27 settembre 2011, *Menarini Diagnostics S.r.l. c. Italia* (ric. n. 43509/08). In base ai criteri Engel, la sentenza emanata nel cd. caso Grande Stevens (Corte EDU, Sez. II, 4 marzo 2014, ricorsi nn. 18640/10 e altri, *Grande Stevens e altri c. Italia*,) ha attribuito natura penale a una sanzione amministrativa pecuniaria irrogata dalla CONSOB in materia di *market abuse*. Dalla qualificazione della sanzione come sostanzialmente penale è derivata la verifica circa il rispetto delle garanzie, previste dall'art. 6, par. 1, CEDU, che avrebbero dovuto essere fornite in sede procedimentale e processuale: il concetto di *full jurisdiction*; la garanzia dell'udienza pubblica; il principio del ne bis in idem.

Legislativo n. 82/2005 (Codice dell'Amministrazione Digitale - CAD) non contiene, a parere di chi scrive, una descrizione sufficientemente specifica delle condotte sanzionate, limitandosi a ritenere sanzionabili i soggetti (Prestatori di Servizi Fiduciari, Gestori di identità Digitali, Gestori di Posta Elettronica Certificata e Conservatori) che "*abbiano violato gli obblighi del Regolamento eIDAS o del presente Codice relative alla prestazione dei predetti servizi*".

4. L'attuale sistema sanzionatorio del Codice dell'Amministrazione Digitale

Il rafforzamento dei poteri di vigilanza dell'Agenzia per l'Italia Digitale e dei correlativi poteri sanzionatori della stessa verso i soggetti sottoposti a vigilanza è avvenuto mediante l'introduzione, nel 2020, dell'art. 14-bis del CAD, 2° comma, lettera i).

Il potere sanzionatorio stabilito in linea generale da tale previsione è regolato nel dettaglio dall'art. 32-bis del medesimo CAD.

La norma prevede diverse tipologie di sanzioni irrogabili dall'Autorità: a) sanzioni pecuniarie; b) sanzioni interdittive (come la cancellazione del fornitore dall'elenco dei soggetti qualificati e il divieto di accreditamento); c) sanzioni accessorie (come la pubblicazione dei provvedimenti di diffida o di cancellazione).

Il richiamo espresso della disciplina della legge 24 novembre 1981, n. 689, in materia di depenalizzazione, evidenzia i punti in comune che hanno le sanzioni stabilite dall'art. 32-bis del CAD con quelle di stampo penalistico

In particolare, l'art. 32 bis del CAD stabilisce:

- delle sanzioni amministrative pecuniarie ai soggetti che "*abbiano violato gli obblighi del Regolamento eIDAS o del presente Codice relative alla prestazione dei predetti servizi*" calcolate, a seconda della gravità della sanzione, da un minimo di 40.000,00 Euro ad un massimo di 400.000,00 Euro (art. 32-bis, 1° comma);
- nel caso di violazioni gravi, ossia a) idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o b) relative a significative carenze infrastrutturali o di processo del fornitore di servizio, in aggiunta alla sanzione pecuniaria ("dispone altresì") AgID può disporre le sanzioni interdittive della cancellazione del fornitore del servizio dall'elenco dei soggetti qualificati e il divieto di accreditamento o qualificazione per un periodo fino ad un massimo di due anni (art. 32-bis, 1° comma, CAD); in entrambe le ipotesi a) e b) AgID può diffidare i soggetti, nel momento in cui adotta il provvedimento sanzionatorio, a conformare la condotta agli obblighi normativi (art. 32-bis, comma 1-bis, CAD);
- nel caso in cui si verifichi un malfunzionamento che determini l'interruzione

del servizio, o in caso di mancata o intempestiva comunicazione dello stesso disservizio a AgID o agli utenti, l'Agenzia può applicare la sanzione pecuniaria e diffidare il soggetto a ripristinare il servizio o ad effettuare le comunicazioni. Se tali condotte sono reiterate nei due anni successivi alla diffida viene applicata la cancellazione dall'elenco (art. 32-bis, comma 2, CAD);

- in tutte le ipotesi appena esaminate può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione (art. 32-bis, comma 3, CAD).

Il potere di vigilanza e sanzionatorio è stato poi ulteriormente disciplinato dalla medesima Autorità con un apposito Regolamento interno (Regolamento recante le modalità per la vigilanza ai sensi dell'art. 14-bis comma 2, lett. i) e per l'esercizio del potere sanzionatorio ai sensi dell'art. 32-bis del d. lgs. 7 marzo 2005, n. 82 - DT 270/2022 - di seguito il "Regolamento"), il quale istituisce i procedimenti che l'ente applica sia per lo svolgimento delle attività di vigilanza sia per l'applicazione delle sanzioni di cui all'art. 32-bis.

In particolare, il procedimento sanzionatorio è regolato dagli articoli da 17 a 20 e prevede una fase di contestazione delle violazioni, una fase istruttoria in cui è garantito il contraddittorio tra le parti, e la fase conclusiva che può terminare con l'archiviazione del procedimento stesso o con l'irrogazione di una sanzione amministrativa pecuniaria (art. 19, 2° comma del Regolamento).

Il 4° comma dell'art. 19 disciplina l'eventuale applicazione delle ulteriori sanzioni (interdittiva o accessoria) stabilendo che con il medesimo provvedimento motivato il Direttore Generale può disporre a) la cancellazione dall'elenco (nei casi di cui all'art. 20); b) l'applicazione della sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida e di cancellazione sul sito istituzionale di AgID, in apposita sezione in evidenza.

Nel caso di definizione del procedimento mediante pagamento in misura ridotta (ai sensi dell'art. 16 della legge n. 689/1981) il Direttore Generale adotta un provvedimento di estinzione del procedimento (art. 19, 6° comma del Regolamento).

L'attuale sistema di gradazione delle sanzioni ruota intorno al sistema delle "non conformità" specificato nel Regolamento interno di AgID. Come sopra descritto l'art. 32 bis stabilisce la potestà sanzionatoria pecuniaria dell'Agenzia nei margini di un importo minimo e di un importo massimo. Oltre a tale tipologia di sanzione vengono individuate alcune circostanze più gravi in cui oltre alla sanzione pecuniarie l'Agenzia ha facoltà di adottare rimedi interdittivi, quali la cancellazione dall'elenco e il divieto di accreditamento.

È evidente, quindi, che un sistema che possa dare evidenza dei criteri adottati per applicare la gradazione della sanzione, anche nel rispetto della L. n. 689/1981, è più che necessario ed è stato individuato nel Regolamento. L'art. 12 introduce un sistema di "non conformità" su tre livelli di gravità: lieve, media e grave.

La prima si verifica quando la violazione sui servizi o sugli utenti non impedi-

sce di continuare l'erogazione del servizio e che può essere risolta con azioni correttive in un termine non superiore a 60 giorni.

Una non conformità "media" si ha invece nei casi in cui la violazione non ostacola la regolare erogazione del servizio e può essere risolta con azioni correttive da attuarsi entro 30 giorni.

Un non conformità "grave" invece non impedisce di continuare l'erogazione del servizio, ma deve essere risolta in un termine massimo di 10 giorni. All'interno di tale tipologia rientrano, ai sensi dell'art. 32 bis del CAD, "*violazioni del presente Codice idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio*".

5. Le questioni applicative del "nuovo" art. 16 alla disciplina di diritto interno

In considerazione della nuova previsione dell'art. 16 che stabilisce, fissando l'importo massimo delle stesse, direttamente nel testo del Regolamento il regime sanzionatorio nei confronti dei prestatori di servizi fiduciari qualificati e non qualificati, e della "delega" espressa agli Stati membri del potere le norme relative alle sanzioni applicabili, nel rispetto dei principi di effettività, dissuasività e proporzionalità, si ritiene che il legislatore italiano sarà chiamato ad intervenire per modificare la previsione oggi contenuta nell'art. 32 bis CAD, con conseguente necessità di intervenire anche sul Regolamento interno adottato da AgID.

Innanzitutto, come sopra anticipato, il legislatore italiano sarà tenuto a specificare in maniera più dettagliata le condotte – comprese quelle indicate nel Considerando 45 - che possono determinare l'applicazione di una sanzione da parte dell'autorità di vigilanza, in quanto l'attuale previsione normativa di dell'art. 32 bis appare, alla luce anche dei criteri dettati dalla giurisprudenza europea e costituzionale, appare eccessivamente generica.

In tal senso, sulla scorta di quanto già compiuto in attuazione di altre norme regolamentari, un rinvio dettagliato agli articoli del Regolamento (e del CAD) la cui violazione può determinare l'applicazione delle sanzioni appare più rispondente ai principi di certezza del diritto, fornendo una sufficiente determinatezza delle condotte dalla cui violazione derivano conseguenze negative per l'agente.

In secondo luogo, l'attuale sistema di gradazione delle sanzioni, basato sul meccanismo delle "non conformità" di cui al Regolamento interno, dovrà necessariamente essere rivisto. Nel complesso delle previsioni del CAD e regolamentari, infatti, non si può non rilevare che in realtà l'attuale normativa italiana non contiene una vera e propria gradazione. Seppur vero che il Regolamento interno di AgID all'art. 12 individua una scala di tre tipologie di non conformità, le stesse non sono ricollegate direttamente alle condotte – dato che in ogni caso è previsto che la violazione non

impedisce di continuare l'erogazione dei servizi – essendo demandata la valutazione di tale gravità esclusivamente alle considerazioni svolte dall'Autorità di controllo.

In tale contesto solamente le condotte più gravi appaiono definite attraverso la previsione normativa di cui all'art. 32 bis del CAD (ossia quelle "*idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore*"), ma i termini utilizzati dalla norma appaiono generici ("significative") e non determinate in senso quantitativo ("pluralità").

Il risultato è che la decisione su come valutare la gravità di una "non conformità" appare demandata alla discrezionalità dell'Autorità e non ancorata a criteri oggettivi predeterminati.

Tale modalità di gradazione appare contraria ai principi di proporzionalità, effettività e dissuasività previsti dal nuovo art. 16, nonché ai principi richiamati dalla L. n. 689/1981 che, all'art. 11 introduce dei criteri specifici per la determinazione delle sanzioni pecuniarie, quali la gravità della violazione, l'opera svolta dall'agente per l'eliminazione o attenuazione delle conseguenze, la personalità del soggetto che ha realizzato la violazione e le sue condizioni economiche.

Di tali aspetti dovrà tener conto il legislatore italiano per provvedere all'adeguamento della normativa interna rispetto alle nuove previsioni contenute nel "nuovo" Regolamento eIDAS.

N. 4 - 2024 - pp. 186-195

Firme Elettroniche Avanzate: Nuovi Riferimenti E Vecchi Problemi Irrisolti

Luigi Foglia

Abstract [IT]: Il Regolamento eIDAS prevede che, entro due anni dalla sua entrata in vigore, la Commissione valuti la necessità di individuare specifiche e procedure per la realizzazione di soluzioni di firma elettronica avanzata. Inoltre, la maggiore attenzione riservata ai fornitori di servizi fiduciari non qualificati suggerirebbe una seria e completa riflessione in materia. In effetti, diventa sempre più concreto il rischio che gli ulteriori requisiti previsti per la realizzazione di FEA dagli artt. 55 e seg. del DPCM 22 febbraio 2013 risultino obsoleti, se non addirittura in contrasto con le specifiche norme UE. Occorre, inoltre, ragionare sui possibili effetti dell'utilizzo delle firme elettroniche avanzate nei servizi offerti online dalle amministrazioni pubbliche alla luce di quanto previsto dall'art. 27 del Reg. EIDAS.

Abstract [EN]: *The eIDAS Regulation requires that, within two years of its entry into force, the Commission evaluates the need to identify specifications and procedures for the creation of advanced electronic signature solutions. Furthermore, the greater attention paid to unqualified trust service providers would suggest a serious and complete reflection on the matter. The risk that the additional requirements envisaged for the creation of FEA by the Prime Minister Decree of 22 February 2013 are obsolete or even in conflict with EU specifications, becomes increasingly concrete. It is also necessary to think about the possible effects of the use of advanced electronic signatures in the services offered online by public administrations in light of the provisions of the art. 27 of the EIDAS Reg.*

Parole chiave: firme elettroniche, prestatori di servizi fiduciari non qualificati, firme elettroniche avanzate, FEA

Sommario: 1. Le modifiche al Regolamento UE 910/2014; 2. Le novità in materia di firme elettroniche; 3. La FEA "italiana" e i requisiti del DPCM 22 febbraio 2013; 4. I nuovi requisiti per i fornitori di servizi fiduciari non qualificati; 5. La FEA nei pubblici servizi; 6. Conclusioni

1. Le modifiche al Regolamento UE 910/2014

Su proposta della Commissione europea, il Parlamento europeo e il Consiglio hanno approvato un nuovo Regolamento che "*modifica il Regolamento (UE) n.*

910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea".

Le modifiche, oltre a concentrarsi sulla definizione di un'identità digitale europea attraverso l'istituzione del Portafoglio europeo d'identità Digitale - EUDI Wallet, hanno anche l'obiettivo, si legge nei lavori della Commissione, di riportare la sovranità dei dati personali nelle mani dei cittadini e garantire parità di condizione nell'utilizzo dei servizi fiduciari all'interno dell'UE.

Inoltre, la Commissione UE, pur riconoscendo che l'applicazione del Regolamento eIDAS abbia garantito livelli elevati di fiducia assicurando l'adozione e l'utilizzo della maggior parte dei servizi fiduciari, ha sottolineato come occorra fare di più per conseguire la piena armonizzazione e accettazione di tali servizi in tutti i paesi membri. Se, infatti, l'Italia è il Paese con la maggiore presenza di fornitori di servizi fiduciari qualificati (QTSP), in alcuni altri paesi la loro presenza è molto limitata.

La Commissione, quindi, si è posta l'obiettivo di aumentare l'interoperabilità e integrabilità dei servizi fiduciari all'interno dell'UE, facendo un ulteriore passo avanti nell'unificazione dei paesi ponendo le basi per creare un reale european digital market.

Infine, per rispondere alle dinamiche dei mercati e agli sviluppi tecnologici, le modifiche al Regolamento eIDAS espandono l'attuale elenco di servizi fiduciari aggiungendo tre nuovi servizi fiduciari qualificati, ossia la prestazione di servizi di archiviazione elettronica, i registri elettronici e la gestione di dispositivi per la creazione di firme e sigilli elettronici a distanza.

2. Le novità in materia di firme elettroniche

Nell'ambito delle modifiche approvate, le firme elettroniche non hanno subito modifiche di particolare rilevanza. In effetti, tra i servizi fiduciari, quelli di firma elettronica sono tra i più diffusi e riconosciuti in ambito UE. Certo, non mancano problemi di verifica delle firme che richiederebbero ulteriori interventi di armonizzazione ma, almeno in tema di firme elettroniche qualificate, si intravede sempre più un reale mercato unico europeo. Queste considerazioni hanno spinto all'introduzione, nel nuovo art. 5 bis del Regolamento, di una lettera g) al paragrafo 5, con la quale è stato previsto che i portafogli europei d'identità digitale offrano a tutte le persone fisiche la possibilità di firmare mediante firme elettroniche qualificate per impostazione predefinita e gratuitamente, dando così seguito al quanto previsto dal considerando 20, il quale suggerisce che "*l'uso di una firma elettronica qualificata dovrebbe essere gratuito per tutte le persone fisiche a fini non professionali, invitando gli Stati membri a prevedere misure che impediscano l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche a fini professionali*".

Sempre in tema di firme elettroniche qualificate, non si può che essere soddisfatti per l'introduzione di specifici "*Requisiti relativi ai servizi qualificati per la*

gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza": con l'introduzione di un nuovo art. 29 bis, il Regolamento 910/2014 riconosce "ufficialmente" la firma remota[1] che, principalmente in Italia, ha avuto un notevole utilizzo contribuendo notevolmente alla diffusione di certificati qualificati in numerosi processi pubblici e privati.

Le firme elettroniche qualificate sono, però, solo una delle tipologie di firma elettronica previste dal Regolamento eIDAS che, fin dalla prima versione definisce tre differenti tipologie di firma elettronica:

1. La "firma elettronica" o "firma elettronica semplice" (simple electronic signature; anche "SES"), definita come "*dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*.
2. La "firma elettronica avanzata" (advanced electronic signature; anche "AES") definita come firma elettronica che soddisfa i seguenti 4 requisiti:
   - *è connessa in modo univoco al firmatario;*
   - *è in grado di identificare il firmatario;*
   - *è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un alto livello di sicurezza, utilizzare sotto il suo esclusivo controllo;*
   - *è collegata ai dati firmati in modo tale da consentire l'identificazione di ogni successiva modifica di tali dati.*
3. La "firma elettronica avanzata basata su un certificato qualificato", è un particolare tipo di firma elettronica avanzata che, seppur non definita in maniera esplicita, viene più volte citata all'interno del Regolamento eIDAS; in Italia non risulta regolamentata in maniera dissimile dalla FEA.
4. La "firma elettronica qualificata" (qualified electronic signature; anche "QES") è infine definita come "*una firma elettronica avanzata creata da un dispositivo per la creazione di firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche*".

In tema di firme elettroniche avanzate le modifiche apportate al Regolamento eIDAS richiedono che la commissione, entro 24 mesi, valuti *la necessità di adottare atti di esecuzione per stabilire un elenco di norme di riferimento e, se necessario, stabilire specifiche e procedure applicabili alle firme elettroniche avanzate*. Sulla base di tale valutazione, la Commissione potrà adottare tali atti di esecuzione, ribadendo che *i requisiti delle firme elettroniche avanzate devono ritenersi rispettati ove una firma elettronica avanzata sia conforme a tali norme, specifiche e procedure*.

A differenza di quanto previsto dal precedente paragrafo 4 dell'art. 27 del

[1] L'art. 1, comma 1, lett. Q) del DPCM 22 febbraio 2013 definisce la firma remota quale: particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;

Regolamento eIDAS[2], viene specificamente richiesto alla Commissione di valutare la necessità di individuare specifiche e procedure applicabili alle firme elettroniche avanzate. Se, infatti, la neutralità tecnologica è sicuramente un principio fondamentale da rispettare, dall'altro lato, la mancanza di specifiche e procedure comuni rende di fatto difficilmente applicabili soluzioni di firma elettronica avanzata all'interno del mercato unico europeo.

3. La FEA "italiana" e i requisiti del DPCM 22 febbraio 2013

L'Italia, con la permanenza in vigore delle regole tecniche di cui al DPCM 22 febbraio 2013, rappresenta l'esempio lampante di come la regolamentazione interna, in assenza di specifiche procedure europee, possa rendere estremamente difficoltoso l'utilizzo di soluzioni di FEA "europee" che possano aspirare ad oltrepassare i confini nazionali. Questo nonostante, con Decisione di esecuzione 1506/2015, la Commissione abbia stabilito le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere.

È bene dirlo subito, la convivenza tra regole italiane e regole europee, quantomeno per le Firme elettroniche avanzate, non è stata mai del tutto pacifica[3]. E lo stratificarsi di previsioni non correttamente adeguate tra loro nel tempo, non ha certamente reso più semplice la corretta interpretazione delle norme in materia. Da anni viene richiesta da numerosi professionisti e associazioni di settore una revisione delle Regole tecniche per l'apposizione delle firme elettroniche, ma nessuno dei Legislatori succedutisi negli ultimi anni ha sentito l'esigenza di portare finalmente chiarezza in un settore delicato e attuale, come quello delle firme elettroniche.

In effetti, ancora oggi, accanto alle disposizioni del Regolamento eIDAS, in tema di modalità di apposizione delle firme elettroniche è necessario far riferimento alle previsioni contenute nel Decreto del Presidente del Consiglio dei ministri del 22 febbraio 2013 contenente le *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.*

---

[2] L'art. 27, paragrafo 4, del Regolamento UE 910/2014 prevedeva che: *La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili alle firme elettroniche avanzate. Si presume che i requisiti per le firme elettroniche avanzate di cui ai paragrafi 1 e 2 del presente articolo e all'articolo 26, siano rispettati ove una firma elettronica avanzata soddisfi dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.*

[3] Basti ricordare come la stessa definizione di Firma elettronica avanzata, in riferimento alla direttiva 99/93/CE che richiedeva un suo esplicito recepimento all'interno del nostro ordinamento, era apparsa nel 2002 (con il D. Lgs. n° 10/2002), per poi sparire nel 2005 ed essere reinserita solo nel 2010.

Come ricordato anche dal considerando 63 al Regolamento di modifica del Regolamento eIDAS, *gli effetti giuridici delle firme elettroniche devono essere stabiliti dal diritto nazionale, salvo per i requisiti previsti dal presente regolamento a norma dei quali gli effetti giuridici di una firma elettronica qualificata devono essere considerati equivalenti a quelli di una firma autografa.*

Inoltre, sempre il citato considerando 63, invita gli Stati membri, nel determinare gli effetti giuridici delle firme elettroniche, a tenere conto del principio di proporzionalità tra il valore giuridico di un documento da firmare e il livello di sicurezza e di costo richiesto da una firma elettronica.

In tal senso, il comma 1-bis dell'art. 20 del D.Lgs 82/2005, così come ridefinito dal D.Lgs. 217/2017, stabilisce, che *"Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata".* Il nostro ordinamento ha quindi ribadito anche nel 2017 l'elevato valore giuridico e probatorio riconosciuto alle firme elettroniche avanzate utilizzabili in tutti i casi in cui sono utilizzabili scritture private, ad eccezione di quelle di cui all'articolo 1350, primo comma, numeri da 1 a 12, del Codice civile, che, se fatte con documento informatico, devono essere sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

Se, però, il D.Lgs. 82/2005 fa riferimento alla definizione di firma elettronica avanzata contenuta nel Regolamento UE 910/2014, il comma 2 dell'art. 56 del citato DPCM 22 febbraio 2013 continua a stabilire che per soddisfare i requisiti di cui all'art. 20 bis del CAD, la firma elettronica avanzata deve rispettare, in aggiunta ai 4 requisiti definiti dal Regolamento eIDAS, 3 ulteriori requisiti:

e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

h) la connessione univoca della firma al documento sottoscritto.

Inoltre, sempre il DPCM 22 febbraio 2013, prescrive che i soggetti che intendono utilizzare soluzioni di firma elettronica avanzata nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, devono:

a. *identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;*
b. *conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilita' e autenticita';*
c. *fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;*

d. *rendere note le modalita' con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;*
e. *rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1;*
f. *specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;*
g. *pubblicare le caratteristiche di cui alle lettere e) e f) sul proprio sito internet;*
h. *assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.*

Inoltre, ai sensi del successivo comma 2 dell'art. 57 del DPCM 22 febbraio 2013, i soggetti che propongono l'utilizzo di una FEA, devono anche dotarsi, al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila.

Infine, sempre con l'obiettivo di limitare i possibili effetti negativi di una soluzione di Firma elettronica non adeguata, l'art. 60 del citato DPCM, prevede che la Firma elettronica avanzata sia utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che propone l'utilizzo della FEA per motivi istituzionali, societari o commerciali.

Il nostro Legislatore ha quindi normato una Firma elettronica avanzata che potremmo definire "rafforzata" rispetto a quella definita in ambito eIDAS e alla quale riconosce sicuramente un elevato valore giuridico e probatorio.

L'art, 21 del D.Lgs. 82/2005, infatti, proprio negli anni di definizione di quello che poi sarebbe stato il DPCM 22 febbraio 2013, prevedeva, senza distinzioni tra FEA e firma digitale, che *L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.*

Questa previsione, poi scomparsa con le modifiche al CAD del 2012[4] e oggi presente nel comma 20 *bis* del CAD solo in riferimento alle firme digitali e qualificate, invertendo l'onere della prova in materia di riconducibilità al Titolare della firma apposta, aveva, forse per eccessiva prudenza, portato a limitare di molto l'utilizzabilità delle FEA.

Ad ogni modo, è bene sottolineare che lo stesso Considerando 63, già citato, conclude incoraggiando gli Stati membri a "*valutare l'uso di firme elettroniche avan-*

[4] Il Decreto Legge 18 ottobre 2012, n. 179 (in SO n.194, relativo alla G.U. 19/10/2012, n.245) convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 ha modificato gli artt. 20, 20 bis e 21 del D.Lgs 82/2005.

zate nelle transazioni quotidiane, per le quali essi forniscono un livello sufficiente di sicurezza e affidabilità".

Speriamo che il nostro legislatore possa cogliere tale invito, eliminando alcuni requisiti ormai eccessivi e procedendo a un coordinamento efficace dell'ormai obsoleto DPCM 22 febbraio 2013 con le attuali prescrizioni europee in materia di firme elettroniche.

4. I nuovi requisiti per i fornitori di servizi fiduciari non qualificati

Tra le novità in materia di Firma elettronica avanzata devono sicuramente essere incluse le più generali novità che hanno un impatto rilevante sui i fornitori di servizi fiduciari. Le modifiche al Regolamento eIDAS prestano particolare attenzione a una più efficiente ed efficace regolamentazione della prestazione dei servizi fiduciari non qualificati.

Un nuovo art. 19 bis introdotto nel Regolamento eIDAS individua i requisiti che i fornitori di servizi fiduciari non qualificati devono soddisfare e sulla sussistenza dei quali i differenti Organismi di Vigilanza (per l'Italia abbiamo L'AgID) dovranno, appunto, vigilare (seppur solo ex post, non essendo prevista alcun tipo di autorizzazione preventiva per la fornitura di servizi fiduciari non qualificati).

L'art. 19 bis prevede, quindi, che "*un prestatore di servizi fiduciari non qualificato che presta servizi fiduciari non qualificati:*

a) dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato, le quali, fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, comprendono almeno misure relative:

i) alla registrazione a un servizio fiduciario e alle relative procedure di onboarding;

ii) ai controlli procedurali o amministrativi necessari per prestare servizi fiduciari;

iii) alla gestione e all'attuazione dei servizi fiduciari;

iv) alla notifica, senza indebito ritardo ma in ogni caso entro 24 ore dall'essere venuto a conoscenza di violazioni della sicurezza o perturbazioni, all'organismo di vigilanza, alle persone interessate identificabili, al pubblico se è di pubblico interesse e, ove applicabile, ad altre autorità competenti interessate, di tutte le eventuali violazioni della sicurezza o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera a), punti i), ii) o iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati

personali ivi custoditi.

Entro 12 mesi dalla data di entrata in vigore del presente regolamento modificativo la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al paragrafo 1, lettera a), del presente articolo".

Dal punto di vista sanzionatorio, il Considerando 44 del Regolamento modificativo del Regolamento eIDAS chiede che vengano stabilite sanzioni amministrative per i prestatori di servizi fiduciari sia qualificati che non qualificati: sanzioni effettive, proporzionate e dissuasive che tengano debitamente in conto delle dimensioni dei soggetti interessati, dei loro modelli di business e della gravità delle violazioni[5].

Risulta interessante anche il richiamo all'art. 21 della direttiva 2555/2022, la cosiddetta Direttiva NIS2: il Considerando 50 ricorda infatti che, a norma della direttiva (UE) 2022/2555, i fornitori di servizi fiduciari sono tenuti ad adottare misure tecniche e organizzative adeguate, quali misure per far fronte a guasti del sistema, errori umani, azioni malevole o fenomeni naturali, per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare minacce informatiche e incidenti significativi conformemente alla medesima direttiva.

Sarà, quindi, di fondamentale importanza verificare come la Direttiva NIS2 sarà recepita dal nostro ordinamento (recepimento che dovrebbe avvenire entro il 17 ottobre 2024) così da definirne tempi e modalità di attuazione anche in relazione alle altre norme ad essa collegate (Cyber Resilience Act, Regolamento DORA, Direttiva CER sui soggetti critici, ecc.).

5. La FEA nei pubblici servizi

In tema di Firma elettronica avanzata è opportuno ricordare anche quanto previsto dall'art. 27 del Regolamento eIDAS. Il Regolamento, infatti, lascia libero ogni stato Membro di stabilire il valore giuridico e probatorio da riconoscere ad un documento sottoscritto con FEA, ma, nel caso in cui uno "*Stato membro richieda una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato di firma elettronica e le firme elettroniche qualificate che almeno siano nei*

[5] Il nuovo art. 16 del Regolamento eIDAS prevede che i singoli Stati membri individuino sanzioni per le violazioni al regolamento pari a un importo massimo di almeno: *a) EUR 5 000 000 se il prestatore di servizi fiduciari è una persona fisica; oppure b) se il prestatore di servizi fiduciari è una persona giuridica, EUR 5 000 000 o pari all'1 % del fatturato mondiale totale annuo dell'impresa a cui apparteneva il prestatore di servizi fiduciari nell'esercizio precedente l'anno in cui si è verificata la violazione, se superiore.*

formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5". Il successivo par. 2 dell'art. 27, stabilisce inoltre che *"Se uno Stato membro richiede una firma elettronica avanzata basata su un certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate basate su un certificato qualificato e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.*

La Commissione europea, con la Decisone di esecuzione (UE) 2015/1506, ha poi stabilito le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere.

Detta Decisione di esecuzione della Commissione europea individua, come firme elettroniche avanzate o qualificate che ogni Stato membro è obbligato a riconoscere, quelle formate rispettando una delle seguenti specifiche tecniche ETSI:

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

La Decisione prevede anche che siano riconosciuti formati di firma elettronica diversi da quelli sopra elencati, a condizione che lo Stato membro in cui è stabilito il prestatore di servizi fiduciari utilizzato dal firmatario offra agli altri Stati membri possibilità di convalida della firma[6], idonee ove possibile al trattamento automatico.

L'obbligo di riconoscimento di firme elettroniche avanzate rischia di diventare decisamente oneroso per lo Stato, considerando che ancora oggi sussistono problemi di effettiva verifica (e conseguente riconoscimento) delle firme qualificate.

---

[6] La decisione di esecuzione 1506/2015 prevede che le possibilità di convalida della firma:

a) permettono agli altri Stati membri di convalidare online, gratuitamente e in modo comprensibile per i non madrelingua, le firme elettroniche ricevute;

b) sono indicate nel documento firmato, nella firma elettronica o nel contenitore del documento elettronico;

c) confermano la validità della firma elettronica avanzata, purché: 1), il certificato associato alla firma elettronica avanzata fosse valido al momento della firma e, qualora la firma elettronica avanzata sia associata a un certificato qualificato, quest'ultimo fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I del regolamento (UE) n. 910/2014, rilasciato da un prestatore di servizi fiduciari qualificato; 2), i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione; 3), l'insieme unico di dati che rappresenta il firmatario sia correttamente trasmesso alla parte facente affidamento sulla certificazione; 4), se al momento della firma è stato utilizzato uno pseudonimo, l'impiego dello pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione; 5), qualora la firma elettronica avanzata sia creata da un dispositivo per la creazione di una firma elettronica qualificata, l'uso di tale dispositivo sia chiaramente indicato alla parte facente affidamento sulla certificazione; 6), l'integrità dei dati firmati non sia stata compromessa; 7), i requisiti di cui all'articolo 26 del regolamento (UE) n. 910/2014 fossero soddisfatti al momento della firma; 8), il sistema utilizzato per convalidare la firma elettronica avanzata fornisca alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consenta di rilevare eventuali questioni attinenti alla sicurezza.

Proprio per evitare di ricadere negli obblighi previsti dall'art. 27 del Regolamento eIDAS, lo stesso DPCM 22 febbraio 2013 all'art. 61, riconoscendo alcune soluzioni di firma elettronica[7] utilizzabili nei confronti delle pubbliche amministrazioni italiane, conteneva il termine "costituiscono soluzioni di Firma elettronica avanzata", poi modificato in "sostituiscono soluzioni di firma elettronica avanzata".

Negli ultimi anni, però, sono state realizzate alcune soluzioni di firma elettronica avanzata utilizzabili nei confronti della Pubblica Amministrazione[8] che rischiano di far scattare l'obbligo previsto dall'art. 27. Anche su questo, l'auspicio è che il Legislatore possa intervenire al più presto adottando regole chiare e puntuali in tema di firme elettroniche avanzate.

6. Conclusioni

Le modifiche al Regolamento eIDAS, pubblicato come 2024/1183 nella Gazzetta Comunitaria il 30 aprile 2024, lasciano pressoché invariato il quadro regolatorio in materia di firme elettroniche. Tuttavia, ciò che appare realmente mutata è l'attenzione alla fornitura dei servizi di firma non qualificata che porta alla necessaria definizione di nuovi requisiti di fornitura sotto il profilo organizzativo e tecnico, con l'obbligo di individuare politiche adeguate ai differenti rischi commerciali, operativi e di sicurezza informatica rilevabili per ogni servizio fiduciario fornito.

In attesa che la Commissione individui le norme di riferimento e, se necessario, stabilisca le specifiche e le procedure applicabili, il nostro Legislatore dovrebbe finalmente affrontare l'annosa questione legata alle attuali regole tecniche per l'apposizione delle firme elettroniche che, già oggi difficilmente applicabili, finiranno per essere inapplicabili o addirittura in contrasto con quanto previsto dalle norme tecniche, dalle specifiche e dalle procedure che la Commissione individuerà.

Ancora una volta, il rischio è quello di non riuscire a rendere competitive in ambito UE le nostre imprese che oggi hanno investito in soluzioni di FEA (sia vendendo proprie soluzioni a terzi che adottandole nei propri processi); inoltre, non andrebbe neanche sottovalutato il rischio, per le nostre PA, di dover riconoscere (con tutte le difficoltà del caso) soluzioni di firma elettronica avanzata realizzate da fornitori di servizi fiduciari stabiliti in altri paesi membri.

---

[7] L'art. 61 del DPCM 22 febbraio 2013 fa riferimento a soluzioni di firma elettronica basate su PEC (facendo riferimento alla cd. PEC id, mai effettivamente realizzata), Carta d'Identità Elettronica, Carta Nazionale dei Servizi, documento d'identità dei pubblici dipendenti (Mod. ATe), passaporto elettronico e altri strumenti ad essi conformi.

[8] Ad esempio, il MIUR ha adottato una soluzione di FEA (https://www.miur.gov.it/-/sigillo-firma-elettronica-avanzata) che, oltre a non sembrare in regola rispetto a quanto previsto dagli articoli 55 e seguenti del DPCM 22 febbraio 2013, obbligherebbe, quantomeno lo stesso ministero, a riconoscere anche altre soluzioni di firma elettronica avanzata conformi alla Decisione di esecuzione 1506/2015.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 196-200

Le nuove regole europee per la sottoscrizione e l'apposizione di sigilli in modalità remota

Giovanni Manca

Abstract [IT]: La cosiddetta firma remota, nata in Italia nel 2009, si è ampiamente diffusa a livello nazionale e comunitario nonostante la mancanza di riferimenti espliciti nel Regolamento europeo 910/2014 (eIDAS). Il nuovo regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea (numerato 2024/1183) introduce un nuovo servizio fiduciario relativo ai dispositivi per la creazione a distanza di firme e sigilli. Questa novità ha impatti sul ciclo di vita di tali apparati (principalmente gli *Hardware Security Module* – HSM) e in particolare sulla loro certificazione di sicurezza, elemento essenziale per le firme e i sigilli qualificati.

Abstract [EN]: The so-called remote signature, born in Italy in 2009, has spread widely at national and Union level despite the lack of explicit references in the European Regulation 910/2014 (eIDAS). The new regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014 regarding the establishment of a framework for a European digital identity (numbered 2024/1183) introduces a new trust service relating to devices for the remote creation of signatures and seals. This innovation has impacts on the life cycle of these devices (mainly the Hardware Security Modules - HSM) and in particular on their security certification, an essential element for qualified signatures and seals.

Parole chiave: eIDAS, servizi fiduciari, firma remota, certificazione, sicurezza.

Sommario: 1. Le modifiche al testo del regolamento – 2. Le prospettive operative – 3. Conclusioni

1. Le modifiche al testo del regolamento

Il nuovo regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea stabilisce importanti novità sul tema della firma remota (e del sigillo remoto). Tale novità è rappresentata da uno specifico e nuovo, rispetto al precedente regolamento, servizio fiduciario che viene definito come:

"*gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza*".

Si può rilevare che nel testo in lingua inglese viene utilizzata la parola *remote* e nel nostro ordinamento esiste la firma remota, ma ovviamente si deve fare riferimento alle traduzioni comunitarie.

Le sopra citate novità sono già nelle premesse, punto (64) e poi nelle definizioni dove sono inseriti i punti 23 bis e 23 ter come riportato di seguito:

(64) Per garantire la coerenza delle pratiche di certificazione in tutta l'Unione, la Commissione dovrebbe emanare orientamenti in materia di certificazione e ricertificazione dei dispositivi qualificati per la creazione di una firma elettronica e dei dispositivi qualificati per la creazione di un sigillo elettronico, anche per quanto riguarda la loro validità e le relative limitazioni temporali. Il presente regolamento non impedisce agli organismi pubblici o privati che dispongono di dispositivi qualificati per la creazione di una firma elettronica certificati di ricertificare temporaneamente tali dispositivi per un breve periodo di certificazione, sulla base dei risultati del processo di certificazione precedente, qualora tale ricertificazione non possa essere effettuata entro il termine stabilito per legge per un motivo diverso da una violazione della sicurezza o da un incidente di sicurezza, fatto salvo l'obbligo di condurre una valutazione delle vulnerabilità e fatta salva la pratica di certificazione applicabile.

"23 bis) "dispositivo qualificato per la creazione di una firma elettronica a distanza", un dispositivo qualificato per la creazione di una firma elettronica che è gestito da un prestatore di servizi fiduciari qualificato conformemente all'articolo 29 bis per conto di un firmatario";

"23 ter) "dispositivo per la creazione di un sigillo elettronico qualificato a distanza", un dispositivo qualificato per la creazione di un sigillo elettronico, che è gestito da un prestatore di servizi fiduciari qualificato conformemente all'articolo 39 bis per conto di un creatore di un sigillo;

L'inserimento di questi concetti prosegue anche nell'articolato dove viene inserito il nuovo articolo 29 bis:

"Articolo 29 bis

Requisiti relativi ai dispositivi qualificati per la gestione di dispositivi

qualificati pr la creazione di una firma remota a distanza

1. *La gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza come servizio qualificato può essere effettuata solo da un prestatore di servizi fiduciari qualificato che:*

a. *Genera o gestisce i dati per la creazione della firma elettronica per conto del firmatario;*
b. *fatto salvo l'allegato II, punto 1, lettera d), può duplicare i dati per la creazione della firma elettronica solo a fini di back-up, a condizione che siano soddisfatti i seguenti requisiti:*
   i. *la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;*
   ii. *il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio.*
c. *soddisfa i requisiti indicati nella relazione di certificazione dello specifico dispositivo per la creazione di una firma a distanza, rilasciata ai sensi dell'articolo 30.*

2. *Entro... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], la Commissione, mediante atti di esecuzione, stabilisce norme di riferimento e, se necessario, specifiche e procedure tecniche ai fini del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2."*

In questo nuovo articolo viene citato l'Allegato II dello schema di regolamento che è utile riportare di seguito con il testo modificato dal nuovo regolamento:

ALLEGATO II
REQUISITI RELATIVI AI DISPOSITIVI QUALIFICATI
PER LA CREAZIONE DELLA FIRMA ELETTRONICA

1. *I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mdiante 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;*
   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 qualificati per la creazione di una firma elettronica non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.*

Per completare l'elenco delle novità su questi nuovi servizi fiduciari deve essere citato anche l'inserimento nell'articolo 30 del paragrafo 3 bis e nell'articolo 31 la sostituzione del paragrafo 3:

> *"3 bis. La validità di una certificazione di cui al paragrafo 1 non supera i 5 anni, subordinatamente a una valutazione periodica delle vulnerabilità ogni 2 anni. Qualora siano individuate vulnerabilità a cui non è posto rimedio, la certificazione è annullata."*
>
> *"3. Entro... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], la Commissione, mediante atti di esecuzione, definisce i formati e le procedure applicabili ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, comma 2."*

2. Le prospettive operative

Completato l'elenco delle novità sui dispositivi per la creazione di firme e sigilli in modalità remota è possibile commentare tali novità.

Alla data non esistono nelle norme primarie o tecniche regole esplicite sui tempi di validità della certificazione dei dispositivi. Una volta che la modifica sarà in vigore e attuabile in seguito degli atti esecutivi della Commissione ci sarà un impatto sul mercato degli HSM. Quelli più "anziani" dovranno essere sostituiti con la nuova generazione di apparati. La disponibilità di nuovi modelli è ampia, quindi sarà solo un problema di attenzione del mercato e della vigilanza istituzionale sul tema. Le regole più stringenti sulla certificazione richiederanno maggiori sforzi da parte dei produttori e maggiori investimenti.

Anche la vigilanza istituzionale (in Italia in capo ad AgID) dovrà modificare le proprie regole di controllo su un tema molto delicato come quello della sicurezza cibernetica della firma remota.

Un aspetto critico è quello delle autorizzazioni all'utilizzo di firma remota con singolo fattore di autenticazione. Le nuove certificazioni *Common Criteria* degli HSM non consentono questa opzione, quindi applicarla significa la perdita della certificazione del dispositivo.

La modifica all'articolo 31 stabilisce tempi rapidi alla Commissione per la definizione di quanto stabilito nell'articolo sulle regole di pubblicazione di un elenco di dispositivi certificati per la creazione delle firme e 12 mesi sono un tempo molto stretto per emettere standard.

Per i sigilli viene introdotto un nuovo articolo 39 bis che riprende le regole per i dispositivi di firma. L'articolo 39 rimane inalterato.

3. Conclusioni

Possiamo concludere con la positiva constatazione che la firma remota (e il sigillo) diventa un servizio fiduciario confermando la visione innovativa nata in Italia quasi quindici anni fa.

Ci si abituerà ad usare i nuovi termini di firma e sigillo "a distanza"

Questa tipologia di firma elettronica e apposizione di sigillo elettronico, si espanderà ulteriormente sfruttando anche le numerose possibilità offerte dalle architetture *cloud* e dallo sviluppo dei *Digital Trust Systems* e del *Digital Transaction Management.*

Per approfondire lo stato attuale mediante una descrizione degli scenari operativi della firma remota si può leggere il testo disponibile al seguente collegamento:

https://www.agendadigitale.eu/documenti/firma-digitale-remota-come-funziona-i-vantaggi-e-i-requisiti/

Un'ultima riflessione sull'interoperabilità degli HSM con il software di firma e apposizione sigillo che si interfaccia con essi. Il software non è interoperabile quindi il legame tra applicazioni ed hardware è vincolante creando anche situazioni di *vendor lock-in*. Questo problema è stato risolto anni fa per le smart card e i token crittografici. Le novità comunitarie descritte suggeriscono di risolvere il problema anche per firme e sigilli remoti.

La specifica tecnica ETSI TS 119 432 è un'ottima candidata a diventare uno standard dopo gli aggiornamenti del caso richiesti per la conformità al nuovo regolamento.

N. 4 - 2024 - pp. 201-207

Il Regolamento 2024/1183 (eIDAS 2.0) e la Firma Elettronica Qualificata: Nuovi scenari e opportunità

Simone Baldini

Abstract [IT]: Il Regolamento 2024/1183 introduce l'European Digital Identity Wallet (EUDIW), un portafoglio digitale europeo che offre nuove opportunità per la gestione dell'identità digitale e la firma elettronica qualificata (FEQ).

L'EUDIW offre maggiore controllo ai cittadini sui propri dati personali, facilita l'accesso a numerosi servizi online e abilita nuovi scenari per la FEQ, come la firma a distanza e su dispositivi mobili.

Nel presente documento verranno analizzate le opportunità e le sfide dell'EUDIW, con particolare attenzione ai modelli di identità digitale, all'utilizzo della FEQ e ai rischi per la privacy e la sicurezza.

L'EUDIW rappresenta un passo avanti significativo per l'identità digitale in Europa. Nel prosieguo si cercherà di evidenziare le implicazioni di questa tecnologia per cittadini, imprese e pubbliche amministrazioni.

Abstract [EN]: The Regulation 2024/1183 introduces the European Digital Identity Wallet (EUDIW), a European digital wallet that offers new opportunities for digital identity management and qualified electronic signatures (QES).

The EUDIW provides citizens with greater control over their personal data, facilitates access to a wide range of online services, and enables new scenarios for QES, such as remote and mobile signing.

This paper will analyze the opportunities and challenges of the EUDIW, with particular attention to digital identity models, the use of QES, and privacy and security risks.

The EUDIW represents a significant step forward for digital identity in Europe. The paper will highlight the implications of this technology for citizens, businesses, and public administrations.

Parole chiave: Firma Elettronica Qualificata (FEQ/QES), Identità digitale, EUDIW (European Digital Identity Wallet), Firma Remota, Riconoscimento, Autenticazione elettronica, Sicurezza, Semplificazione, Opportunità.

Sommario: 1. Antefatti e contesto - 2. Scenario attuale – 3. Lo European Digital Identity Wallet (EUDIW) - 4. Possibilità offerte e opportunità per nuovi flussi digital – 5. Nuovi scenari di rilascio – 6. Nuovi scenari per la sottoscrizione dei documenti – 7. Conclusioni

1. Antefatti e contesto

Il Regolamento eIDAS[1] "Regolamento UE n° 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE" (nel prosieguo eIDAS o Regolamento), adottato dall'Unione Europea nel 2014, mirava a semplificare le transazioni elettroniche sicure all'interno del mercato unico. Prima di eIDAS, il panorama dei servizi di identificazione elettronica e firma digitale risultava frammentato e disomogeneo a causa di normative nazionali disparate, ostacolando l'interoperabilità e l'adozione diffusa di queste tecnologie.

Con l'introduzione del Regolamento, si è creato un quadro normativo armonizzato, superando tali barriere e definendo regole comuni per l'identificazione elettronica, la firma elettronica (creazione e convalida), i sigilli elettronici (creazione e convalida), le validazioni temporali elettroniche (comunemente note come marche temporali), servizi elettronici di recapito certificato, creazione e convalida di certificati di autenticazione web e conservazione di firme, sigilli o certificati elettronici relativi ai servizi appena indicati.

eIDAS ha avuto un impatto significativo sull'adozione della firma elettronica in Europa, soprattutto per la firma elettronica qualificata (FEQ/QES), che assicura un livello di sicurezza equiparabile alla firma autografa e che è diventata strumento fondamentale in vari settori, come la pubblica amministrazione, la finanza e il commercio elettronico.

2. Scenario attuale

Grazie alla sempre più diffusa adozione della firma elettronica (in particolar modo quella qualificata) si sono potuti ottenere numerosi benefici, tra cui:

- Maggiore efficienza: La firma elettronica elimina la necessità di stampare, firmare e spedire documenti cartacei, velocizzando i processi e riducendo i costi;
- Migliore sicurezza: la firma elettronica (specie quella qualificata) offre un elevato livello di sicurezza grazie all'utilizzo di tecnologie crittografiche avanzate che garantiscono l'integrità e l'autenticità dei documenti restando al passo con i tempi rispetto alle evoluzioni tecnologiche;
- Maggiore usabilità: la firma elettronica consente di sottoscrivere documenti digitali da qualsiasi luogo e in qualsiasi momento, favorendo l'inclusione digitale.

[1] https://www.agid.gov.it/it/piattaforme/eidas

Sebbene il successo di eIDAS abbia aperto la strada a ulteriori sviluppi nel campo dell'identificazione elettronica, firma elettronica e più in generale quello dei servizi fiduciari, la sua adozione, con particolare riferimento al dominio delle identità elettroniche, non ha ottenuto il risultato sperato.

Sebbene il successo di eIDAS abbia indubbiamente spianato la strada a progressi notevoli nel campo dell'identificazione elettronica, della firma digitale e, più in generale, dei servizi fiduciari, la sua adozione, soprattutto in riferimento al dominio delle identità elettroniche, ma anche delle FEQ, non ha raggiunto i risultati sperati.

In relazione al settore della Firma Elettronica Qualificata le ragioni di questa disomogeneità sono molteplici. Innanzitutto, le FEQ europee non sono tutte uguali: le differenti modalità di verifica e autenticazione adottate dai vari Stati membri hanno creato confusione e ostacolato l'interoperabilità transfrontaliera. A ciò si aggiunge la scarsa conoscenza da parte degli utenti delle diverse procedure di verifica, che ha contribuito a limitare l'utilizzo delle FEQ.

L'Italia rappresenta un'eccezione ed un'eccellenza in questo panorama. Le FEQ, infatti, sono largamente utilizzate nel nostro Paese, grazie anche all'implementazione di sistemi di verifica semplici e intuitivi e ad una maturità tecnologica, funzionale e normativa frutto di un costante impegno profuso negli ultimi 20 anni. Tuttavia, in altri Stati membri la diffusione delle FEQ è ancora limitata, con notevoli disparità tra i vari Paesi.

È evidente, dunque, che per realizzare un vero e proprio mercato unico digitale europeo è necessario superare le barriere che ancora ostacolano l›adozione diffusa delle FEQ. L›armonizzazione delle procedure di verifica e autenticazione, insieme a campagne di sensibilizzazione mirate, potrebbero contribuire a rendere le FEQ uno strumento realmente utile e fruibile per tutti i cittadini europei.

Per i motivi sopra indicati, il 3 giugno 2021, la CE (Comunità Europea) ha avviato i lavori sul nuovo regolamento, con lo scopo di aggiornare il quadro normativo esistente introducendo nuove disposizioni per rafforzare la sicurezza e l'interoperabilità dei servizi digitali.

Il testo del nuovo regolamento è stato pubblicato sulla Gazzetta Ufficiale della Comunità Europea il 30 aprile 2024 ed è numerato come 2024/1183 (nel seguito eIDAS 2.0).

3. Lo European Digital Identity Wallet (EUDIW)

Uno degli aspetti più innovativi di eIDAS 2.0 è l'introduzione dello European Digital Identity Wallet (EUDIW), un portafoglio digitale europeo che consentirà ai cittadini di archiviare e utilizzare in modo sicuro le proprie identità digitali e i propri dati personali per accedere a una vasta gamma di servizi online che verranno resi disponibili in tutta Europa.

L'EUDIW sarà un'App sotto il pieno controllo dell'utente, sicura ed interope-

rabile offrirà ai cittadini un maggiore controllo sui propri dati personali e faciliterà l'accesso a servizi online, quali:

- Servizi della pubblica amministrazione: accesso a portali e servizi online, richiesta di documenti, servizi di pagamento e possibilità di firmare elettronicamente istanze e documenti.
- Servizi finanziari: apertura di conti correnti, richiesta di prestiti, firma di contratti online.
- Servizi di commercio elettronico: acquisto di beni e servizi online, autenticazione su siti web e app.

L'EUDIW è previsto per il 2025 e rappresenta un passo avanti significativo nell'evoluzione del sistema eIDAS. Il portafoglio di identità digitale europeo avrà un impatto positivo sulla vita dei cittadini, delle imprese e delle pubbliche amministrazioni, favorendo la creazione di un ecosistema digitale europeo più sicuro e interoperabile.

4. Possibilità offerte e opportunità per nuovi flussi digital

eIDAS 2.0 offre nuove opportunità per la creazione di flussi digitali completamente dematerializzati in diversi settori. La semplificazione delle procedure di identificazione e firma elettronica avrà un impatto positivo sull'efficienza e la competitività delle aziende europee afferenti al settore pubblico e privato.

Alcuni esempi di nuovi flussi digitali abilitati da eIDAS 2.0 includono:

- Firma a distanza di contratti: i cittadini e le imprese potranno sottoscrivere contratti digitali da qualsiasi luogo e in qualsiasi momento, senza la necessità di incontrarsi di persona. Questo scenario, già in parte reso possibile dall'attuale Regolamento eIDAS 1.0, sarà reso ancora più resiliente, sicuro ed interoperabile con l'attuazione di eIDAS 2.0 portando grandi vantaggi per le aziende che operano a livello internazionale, in quanto si andrà verso una più marcata eliminazione della necessità di spostamenti fisici o di utilizzo di procedure complicate per la firma dei documenti.
- Apertura di conti correnti online: i cittadini potranno aprire conti correnti online in modo rapido e sicuro, senza la necessità di recarsi in filiale. L'identificazione elettronica e la firma elettronica qualificata, **fruite tutte all'interno dello stesso strumento (smartphone con singola App)** garantiranno sicurezza, autenticità ma soprattutto **semplicità** del processo.
- Richiesta di prestiti online: i cittadini e le imprese potranno richiedere prestiti online in modo semplice e veloce, grazie all'utilizzo di firme elettroniche qualificate e di sistemi di identificazione elettronica che semplificano

l'accesso al credito. Anche qui con un'unica App.

- Accesso a servizi online della pubblica amministrazione: i cittadini potranno accedere a una vasta gamma di servizi online della pubblica amministrazione, come il pagamento di tasse e multe, la richiesta di documenti e l'accesso a portali informativi, utilizzando le loro identità digitali e le firme elettroniche.

5. Nuovi scenari di rilascio

eIDAS 2.0 promette l'introduzione di nuovi scenari per il rilascio di firme elettroniche qualificate, ampliando le possibilità e il grado di flessibilità per cittadini, imprese e pubblica amministrazione.

Oltre ai tradizionali sistemi di firma basati su smart card e token USB, nonché di identificazione e rilascio, quest'ultimi effettuati tramite canonici processi in presenza e/o video call più o meno automatizzate, eIDAS 2.0, grazie all'introduzione dell'EUDIW, apre la strada alle seguenti novità:

- Firma elettronica qualificata realmente basata su cloud: i cittadini e le imprese potranno ottenere firme elettroniche qualificate da qualificatori di firma basati su infrastrutture cloud, senza la necessità di installare software o dispositivi aggiuntivi. Questo modello offre maggiore flessibilità e accessibilità, in quanto permette di utilizzare la firma elettronica da qualsiasi dispositivo connesso a Internet. Grazie all'introduzione dell'EUDIW e all'adozione di flussi di firma remota maggiormente integrati, e soprattutto interoperabili con i nuovi schemi di identificazione elettronica e strong authentication resi disponibili dall'EUDIW, ogni utente (privato e non) potrà apporre comodamente la propria firma elettronica qualificata con processi interamente basati su paradigmi full mobile (o ibridi) senza la necessità di dover gestire ulteriori attività amministrative o di set-up: con poche azioni dell'utente, interamente effettuate sull'EUDIW e orientate ad acquisire il consenso e preservare il principio del WYSIWYS (What You See Is What You Sign), sarà possibile apporre la firma elettronica qualificata su qualsiasi documento.
- Firma elettronica qualificata su dispositivi mobili: eIDAS 2.0 apre la strada all'utilizzo di firme elettroniche qualificate su dispositivi mobili, come smartphone e tablet. Questo scenario è particolarmente vantaggioso per gli utenti che necessitano di sottoscrivere documenti digitali in mobilità, anche in contesti offline.
- Firma elettronica qualificata remota: eIDAS 2.0 introduce un nuovo servizio fiduciario per *la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza*. Grazie all'entrata in gioco di questo nuovo servizio fiduciario

sarà possibile far affidamento su nuovi modelli di erogazione della firma elettronica qualificata remota che garantiscano standard di sicurezza omogenei per la parte afferente alla gestione dei dispositivi di firma remota (denominati anche come r-QSCD - remote Qualified Signature Creation Device) e, soprattutto, modelli di fruizione del servizio realmente interoperabili..

6. Nuovi scenari per la sottoscrizione dei documenti

eIDAS 2.0 rivoluziona la sottoscrizione dei documenti digitali, offrendo maggiore flessibilità, sicurezza e affidabilità per cittadini e imprese. Oltre alla firma elettronica qualificata tradizionale, eIDAS 2.0 introduce due nuovi scenari che semplificano i processi e ne ampliano l'utilizzo:

- Firma ovunque, in qualsiasi momento: Con la firma remota, cittadini e imprese possono sottoscrivere documenti digitali da remoto, in tempo reale e da qualsiasi dispositivo, tramite sistemi di firma elettronica remota e identificazione elettronica.
  Tra i vantaggi spiccano: la possibilità di effettuare transazioni internazionali veloci e fluide, firma in mobilità, ovunque ci si trovi e maggiore flessibilità per utenti e aziende
- Esperienza fluida ed intuitiva: eIDAS 2.0 permette di firmare documenti digitali su tablet e smartphone, anche tramite l'App dell'EUDIW. Un'unica app per un'esperienza di firma semplice e accessibile a tutti.
  Grazie ad un unico journey di firma, L'esperienza utente viene ottimizzata, facilitata e velocizzata su dispositivi mobili.
- Esperienza one-shot: eIDAS 2.0 facilita l'adozione della firma digitale grazie a un processo semplificato che integra emissione del certificato e firma in un unico passaggio, ideale per le sottoscrizioni occasionali. Questo approccio, denominato "one-shot", aumenta l'usabilità e la diffusione della firma digitale, favorendo la dematerializzazione dei processi e la digitalizzazione dei business.
- Valorizzazione degli attributi qualificati del firmatario: eIDAS 2.0, introducendo il servizio fiduciario di attestazione degli attributi, permette di appoggiarsi all'uso delle cosiddette attestazioni elettronica qualificate di attributi (Qualified Electronic Attribute Attestation - QEAA) per arricchire le firme elettroniche qualificate associandogli informazioni aggiuntive afferenti il firmatario, quali ruolo, qualifiche e altri attributi professionali, che possono snellire ed efficientare in modo rilevante determinati processi di business o flow documentali.
  I vantaggi raggiungibili in questo caso vanno da una maggiore affidabilità e sicurezza delle transazioni online ad una semplificazione dei processi di

verifica (assieme alla firma viaggiano maggiori informazioni qualificate che possono aiutare ad automatizzare logiche decisionali) fino ad arrivare a nuove opportunità per la firma in contesti professionali.

L'introduzione di questi nuovi scenari di sottoscrizione avrà un impatto positivo sull'efficienza e la competitività delle aziende europee (sia del settore privato che pubblico), favorendo l'adozione di modelli di business digitali e la dematerializzazione dei processi.

7. Conclusioni

eIDAS 2.0 rappresenta un passo avanti significativo per la Firma Elettronica Qualificata (FEQ). Le nuove disposizioni del Regolamento rafforzano la sicurezza e l'interoperabilità della FEQ, aprendo la strada a nuovi scenari di utilizzo.

In particolare, eIDAS 2.0 introduce:

- Nuovi modelli di rilascio della FEQ: la firma elettronica qualificata potrà essere ottenuta da qualificatori di firma basati su infrastrutture cloud e su dispositivi mobili;
- Nuovi scenari di sottoscrizione: la FEQ potrà essere apposta su documenti a distanza, su tablet e smartphone
- Maggiore flessibilità e accessibilità: la FEQ sarà più facile da utilizzare e accessibile a un maggior numero di cittadini e imprese.

L'impatto di eIDAS 2.0 sulla FEQ sarà positivo, poiché:

- Aumenterà l'adozione della FEQ: la semplificazione delle procedure e la maggiore flessibilità d'uso favoriranno l'utilizzo della FEQ in diversi settori.
- Migliorerà la sicurezza e l'affidabilità della FEQ: i nuovi requisiti di sicurezza e l'interoperabilità garantiranno un livello di sicurezza elevato per la FEQ.
- Promuoverà l'innovazione: l'introduzione di nuovi modelli di rilascio e di sottoscrizione stimolerà l'innovazione nel campo della FEQ.

N. 4 - 2024 - pp. 208-222

Le procedure di identificazione del titolare nel Regolamento 2024/1183 (eIDAS 2): prospettive europee e nazionali

Igor Marcolongo

Abstract [IT]: Il Regolamento 2024/1183 (eIDAS 2) innova profondamente le regole in merito alle modalità di identificazione del titolare, che i Prestatori di Servizi Fiduciari Qualificati devono mettere in atto per l'emissione di certificati qualificati, estendendole anche ai processi di emissione di attributi qualificati e attivando processi di standardizzazione tecnica e funzionale.

Il nuovo articolo 24 avrà un impatto importante sui processi dei Prestatori di Servizi Fiduciari Qualificati e sui costi aggiuntivi che se ne origineranno, nonché sull'omogeneizzazione degli approcci in ambito europeo e sul mercato dei certificati qualificati: nell'articolo si tenterà una disamina delle modalità di riconoscimento ammesse e degli impatti connessi, ipotizzando possibili scenari di mercato.

Abstract [EN]: The Regulation 2024/1183 (eIDAS 2) innovates deeply the rules around the identification methods of the holder of a Qualified Certificates that the Qualified Trust Service Providers shall respect, extending it even to the processes for issuing qualified attestations of attributes, and enabling technical and functional standardization.

The new article 24 will impact the operative processes of QTSPs, creating additional costs, and has the potential to harmonize the approaches in the different European markets for trust services: this paper deeps dive the different allowed identification methods and the related impacts, trying to predict possible market scenarios.

Parole chiave: eIDAS, Regolamento, firma digitale, firma qualificata, firma avanzata, certificato, certificato di firma, certificatori, QTSP, identità digitale, identificazione, standard, ETSI, attributi, wallet, portafoglio, attestati di attributi

Sommario: 1. Introduzione – 2. La proposta iniziale della Commissione Europea – 3. Il nuovo regime per la verifica dell'identità – 4. La verifica degli attributi – 5. Gli atti di esecuzione e le misure transitorie – 6. Gli impatti sul mercato dei QTSP: alcune previsioni

1. Introduzione

Nella disamina del testo di revisione del Regolamento UE n. 910/2014, noto anche come Regolamento eIDAS, i Prestatori Qualificati di Servizi Fiduciari (QTSP) hanno una particolare attenzione sull'articolo 24 e le innovazioni portate. L'articolo 24, infatti, impatta in maniera importante sull'operatività e la competitività di un QTSP, in quanto fornisce il quadro, i requisiti e i limiti all'interno dei quali esso può definire i processi di identificazione del titolare del certificato qualificato, probabilmente la fase che maggiormente plasma l'esperienza del cliente. Nel mercato odierno le aziende competono per attrarre l'attenzione dei clienti, fornendo loro un'esperienza memorabile: un processo più o meno accattivante può fare la differenza tra il successo, e quindi la profittabilità, e l'insuccesso commerciale.

L'Italia è uno dei Paesi europei che ha saputo costruire un mercato del *digital trust* maggiormente competitivo, in particolare nel segmento della firma qualificata, con grandi imprese capaci di competere anche a livello internazionale con processi innovativi e la capacità di diffondere lo strumento della firma qualificata in numerosi settori. Le cause di questo successo sono molteplici, non da ultima una capacità dei QTSP stessi e dell'Autorità di Vigilanza AgID di interpretare i requisiti dettati dall'articolo 24 del Regolamento in maniera coerente con le esigenze di business costruendo processi di identificazione *user friendly*, senza perdere in sicurezza e affidabilità del processo. Ciò, unito alla regolamentazione della firma a distanza – o firma remota – e all'emergere di processi di firma basati su un certificato *short-term*[1], hanno reso la sottoscrizione mediante certificato qualificato quasi uno standard di mercato in numerosi casi d'uso, soprattutto in contesto B2B2C[2], come la sottoscrizione di contratti nel settore del credito al consumo o i processi di apertura di rapporti a distanza nel settore finanziario (il cosiddetto *onboarding*).

La formulazione finale del testo dell'articolo 24 rispecchia in ogni caso la volontà del legislatore di rafforzare la certezza dell'identità di un titolare di certificato

---

[1] La norma tecnica ETSI EN 319 411-1 definisce come "*short-term certificate: certificate whose validity period, i.e. the period of time from not Before through not After, inclusive, is shorter than the maximum time to process a revocation request as specified in the certificate practice Statement*". Si tratta di certificati di sottoscrizione, definiti anche *One Shot* o *on-the-fly*, con una durata molto contenuta che di fatto li rende utilizzabili per la generazione di firme in una sessione specifica, che quindi sgravano il titolare da una serie di adempimenti di gestione del certificato stesso.

[2] "*Sigla di* Business to business to consumer. *Transazione in cui un'impresa vende un servizio o un prodotto a un consumatore, utilizzando come intermediario un'altra impresa, che può essere costituita da una piattaforma di trading online. Tale tipologia di commercio si è infatti diffusa particolarmente con l'avvento di Internet. In questo modello distributivo, il produttore raggiunge quindi il cliente finale non direttamente, ma coinvolgendo i propri distributori (può aprire canali diretti con il cliente, senza però estromettere l'intermediario dal processo di business). La prima B della sigla si riferisce dunque al venditore su larga scala (per es. un produttore di beni o servizi), la seconda B si riferisce alla piattaforma online o comunque all'intermediario, mentre la C si riferisce all'acquirente. L'intermediario può aumentare il valore aggiunto, mediante servizi offerti, gestione dei clienti, feedback informativi, gestione dei dati, funzioni a supporto delle decisioni*.". Da Enciclopedia Treccani, Lessico del XXI Secolo (2012).

qualificato e di aspirare all'armonizzazione delle modalità di identificazione tra i diversi Stati Membri, fornendo un quadro di interpretazione omogeneo alle Autorità di Vigilanza deputate ad approvare i Rapporti di Conformità (CAR – *Conformity Assessment Report*) emessi dagli Organismi di Certificazione (CAB – *Conformity Assessment Body*), chiamati a valutare l'aderenza dei processi promossi dai QTSP con i principi e gli obiettivi del Regolamento. Una scelta che, come si vedrà qui di seguito, ha suscitato accese reazioni da parte degli *stakeholder* di mercato e che avrà non pochi impatti sulla configurazione dei processi di emissione dei certificati nel medio e nel lungo termine nonché sicure ripercussioni anche sul progetto del Portafoglio di Identità Digitale EUDI.

2. La proposta iniziale della Commissione Europea

La proposta iniziale di revisione del Regolamento presentata dalla Commissione prevedeva un aggiornamento dell'articolo 24, senza tuttavia innovazioni dirompenti:

Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:
'1. When issuing a qualified certificate or a qualified electronic attestation of attributes for a trust service, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued.
The information referred to in the first subparagraph shall be verified by the qualified trust service provider, either directly or by relying on a third party, in any of the following ways:

a) by means of a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high';
b) by means of qualified electronic attestations of attributes or a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d);
c) by using other identification methods which ensure the identification of the natural person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;
d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws if other means are not available.';

(b) the following paragraph 1a is inserted:
'1a. Within 12 months after the entry into force of this Regulation, the

Commission shall by means of implementing acts, set out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with paragraph 1, point c. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'; [3]

Prima di passare alla disamina della versione finale del testo condiviso, è interessante notare alcuni aspetti che evidenziano come la Commissione avesse ben chiaro come nell'applicazione di eIDAS la firma qualificata fosse stata un successo e l'articolo 24 necessitasse di una più accurata riflessione e di un aggiornamento, ma senza alterarne i concetti di base.

Balza subito agli occhi l'estensione dello scopo dell'articolo, prima riferito esclusivamente ai certificati qualificati (di sottoscrizione, di sigillo, di autenticazione ai siti web) e ora esteso anche al nuovo servizio fiduciario di attestato elettronico di attributi qualificato, al fine di regolamentare anche le verifiche connesse al nuovo servizio proposto.

Inoltre, la Commissione proponeva di cambiare l'ordine in cui i metodi di identificazione ammessi erano raccontati: al primo punto descrive i mezzi di identità digitale notificati dagli Stati Membri (prima descritti per secondi, alla lettera b), mentre le modalità di verifica dell'identità in presenza secondo le normative nazionali sono ora dettagliate come ultima opzione, quasi a voler dare un'indicazione impli-

---

[3] In assenza di una traduzione ufficiale della proposa originaria, si presenta di seguito una traduzione ufficiosa dell'articolo:
L'articolo 24 viene modificato come segue:
(a) il paragrafo 1 viene sostituito dal seguente:
'1. Allorché rilascia un certificato qualificato o un'attestato elettronico di attributi qualificato per un servizio fiduciario, un fornitore di servizi fiduciari qualificato deve verificare l'identità e, se applicabile, eventuali attributi specifici della persona fisica o giuridica a cui viene rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.
Le informazioni di cui al primo comma sono verificate dal fornitore di servizi fiduciari qualificato, direttamente o ricorrendo a un terzo, in uno dei seguenti modi:
a) mediante un mezzo di identificazione elettronica notificato che soddisfa i requisiti stabiliti nell'articolo 8 per quanto riguarda i livelli di garanzia 'significativo o 'elevato;
b) mediante attestati elettronici di attributi qualfiicati o un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciati a norma della lettera (a), (c) o (d);
c) mediante altri metodi di identificazione che assicurano l'identificazione della persona fisica con un elevato livello di fiducia, la cui conformità deve essere confermata da un organismo di valutazione della conformità;
d) mediante la presenza fisica della persona fisica o di un rappresentante autorizzato della persona giuridica mediante procedure appropriate e in conformità con le leggi nazionali se non sono disponibili altri mezzi.'.

(b) viene inserito il seguente paragrafo 1a:
'1a. Entro 12 mesi dall'entrata in vigore di questo regolamento, la Commissione, mediante atti di esecuzione, stabilisce specifiche tecniche minime, norme e procedure relative alla verifica dell'identità e degli attributi in conformità con il paragrafo 1, punto c. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 48(2).'.

cita di essere un caso residuale. Sensazione rafforzata dalla proposta, poi espunta dal testo, di ricorso all'identificazione in presenza solo "se non sono disponibili altri mezzi", segnale di una implicita preferenza della Commissione per il ricorso a sistemi di riconoscimento a distanza, forse perché considerati più sicuri, tracciabili e scevri da condizionamenti rispetto all'incontro fisico.

Ancora, in merito al livello di garanzia (nel seguito anche LoA, *Level of Assurance* come definito dal testo in inglese) richiesto per i mezzi di identità digitale ammessi, la Commissione proponeva di confermare l'opzione per i QTSP di ricorrere a un LoA significativo (*substantial*) o elevato (*high*). L'articolo proposto inoltre non citava il portafoglio europeo di identità digitale, in quanto esso era definito in proposta come mezzo di identità digitale; pertanto, era già ricompreso nella categoria generale, con la facoltà per il QTSP di scegliere se ricorrervi con LoA significativo o elevato.

Il paragrafo 1a, in linea con le risultanze dello studio sulla valutazione dell'applicazione del Regolamento eIDAS (il cd. *impact assesment*) svolto prima della formulazione della proposta[4], andava inoltre a introdurre l'obbligo per la Commissione di emanare uno o più atti di esecuzione al fine di armonizzare gli approcci dei diversi CAB e Autorità di vigilanza mediante la definizione di specifiche tecniche minime, norme e procedure relative alla verifica dell'identità e degli attributi, previsione che vedremo è stata confermata dal testo finale.

3. Il nuovo regime per la verifica dell'identità

Il risultato del dibattito tenutosi in particolar modo in seno al comitato ITRE del Parlamento Europeo, insieme al lavoro di affinamento dei testi svolto dalle diverse Presidenze di turno del Consiglio Europeo e a valle dei dibattiti e delle decisioni assunte in fase di Trilogo, è un articolo 24 del Regolamento eIDAS profondamente

[4] L'esigenza di una armonizzazione di approccio è evidenziata a pagina 108 nel documento "*Evaluation study of the Regulation no. 910/2014 (eIDAS Regulation) SAMRT 2019/0046 Final Report*", pubblicato sul sito della Commissione Europea al link https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-evaluation-regulation: "*Several stakeholders consulted noted that the reference in Article 24(1)(d) to the use of "other identification methods recognised at national level" is inappropriate as* ***the implementation of this notion diverges from Member State to Member State. Stakeholders called for a common understanding among Member States of this notion. This could be achieved by the issuance of further guidance as regards the verification by TSP of the specific attributes of the person to the whom the qualified certificate is issued.***
The requirements for qualified trust service providers would be more consistent across the EU if these requirements were further harmonised. For example, either physical presence is required in all cases or it is not, and if 'other identification means' can be relied on, these should be the same across all Member States. Going further, should it be explicitly clarified that physical presence is not required, the rules for remote identification would need to be introduced in order to guard against divergences. This would mean that the verification required by Article 24(1) would be more harmonised across all Member States."

novellato:

l'articolo 24 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

1. Allorché rilascia un certificato qualificato o un attestato elettronico di attributi qualificato, un prestatore di servizi fiduciari qualificato verifica l'identità e, se opportuno, eventuali attributi specifici della persona fisica o giuridica a cui deve essere rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

1 bis. La verifica dell'identità di cui al paragrafo 1 è effettuata, con mezzi adeguati, dal prestatore di servizi fiduciari qualificato, direttamente o tramite un terzo, sulla base di uno dei metodi seguenti o, ove necessario, di una combinazione degli stessi, conformemente agli atti di esecuzione di cui al paragrafo 1 quater:

a. mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato;

b. mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato conformemente alla lettera a), c) o d);

c. mediante altri metodi di identificazione che garantiscono l'identificazione della persona con un elevato livello di sicurezza, la conformità dei quali è confermata da un organismo di valutazione della conformità;

d. mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale.

Nel testo finale si conferma l'estensione del campo di applicazione dell'articolo 24 che, oltre a regolamentare le modalità di identificazione per l'emissione di certificati qualificati, va ad occuparsi anche degli attestati elettronici di attributi qualificati. In questo paragrafo si approfondiranno le innovazioni relative ai certificati qualificati, lasciando al prossimo le analoghe disposizioni sulla verifica degli attributi.

La norma prevede che il QTSP debba procedere alla verifica dell'identità "*con mezzi adeguati*": aggiornando quindi la formulazione "*mediante mezzi appropriati e conformemente al diritto nazionale*" presente nel Regolamento del 2014. Non si ritiene che questa evoluzione abbia particolari conseguenze concrete, ma si rileva come sia invece sparito dal primo comma il riferimento al diritto nazionale, che ritroviamo invece solamente *oltre*, come dettaglio della modalità tipizzata dalla lettera d) che regolamenta l'identificazione mediante presenza concreta della persona fisica, quasi come ad indicare che questo è l'unico metodo dove la normativa nazionale potrà dare indicazioni specifiche (ad esempio sul ruolo del Pubblico Ufficiale, del Notaio, o di altre figure analoghe).

Diventa quindi facile, considerando anche la previsione futura di un atto di

esecuzione che dettaglierà le modalità tecniche e operative da rispettare (si veda il comma 4-ter, commentato *oltre*), giungere alla conclusione che la garanzia di adeguatezza dei mezzi impiegati dal QTSP è assolta con il rispetto pedissequo di quanto previsto dall'atto di esecuzione, previsione che non lascia particolari margini di flessibilità agli Stati Membri rispetto ai metodi di identificazione tipizzati.

Venendo ai suddetti metodi di identificazione, il novellato articolo di fatto conferma l'impianto precedente, pur integrandolo e confermando il nuovo ordine di esposizione dei metodi già presente nella proposta della Commissione.

Il primo metodo descritto alla lettera a) dispone la facoltà di utilizzo del **portafoglio europeo di identità digitale** oppure di **mezzi di identificazione elettronica notificati**: la novella in questo caso, oltre alla previsione di EUDI, è il livello di garanzia che è innalzato da *significativo* a *elevato*. Poiché anche l'articolo 5-bis, comma, 5 lettera d. specifica chiaramente che i portafogli europei di identità digitale "*soddisfano i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato, in particolare in relazione ai requisiti per il controllo e la verifica dell'identità e alla gestione e autenticazione dei mezzi di identificazione elettronica*", viene da sé che la lettera a) ammette solo ed esclusivamente il LoA elevato.

Una scelta che ha scatenato una accesa discussione[5] in quanto ritenuta in grado di incidere negativamente sulla diffusione stessa dei certificati qualificati. La voce più forte si è alzata a febbraio 2023, nel pieno del dibattito di Consiglio, con l'azione del consorzio internazionale *CSC – Cloud Signature Consortium*, supportato dalle principali organizzazioni dei QTSP europei, che ha diffuso una lettera aperta a tutti i *policymaker*[6]. Nella lettera le associazioni sottolineavano che le identità digitali più utilizzate in Europa sono con livello di garanzia significativo e offrono ai cittadini sicurezza e facilità d'uso. Gli esempi portati a supporto sono lo SPID in Italia, ma anche BankID e FrejaID+ in Svezia, il sistema danese NemID/MitID e il sistema FranceConnect. La lettera sottolineava, inoltre, che i Paesi dotati di uno schema di eID con LoA significativo hanno costruito valore per i cittadini e un ambiente fertile ai QTSP per l'emissione di certificati qualificati, migliorando il livello generale di sicurezza delle transazioni elettroniche. Gli schemi con LoA elevato basati su carte con chip come la CIE in Italia e la *Personalausweis* in Germania, invece, hanno un utilizzo più limitato: il dato presentato ha sottolineato che, nonostante oltre 60 mi-

---

[5] Si veda ad esempio la lettera aperta di Jon Ølnes, Tribe Lead sign and trust services at Signicat AB titolata "*Dear EU Commission, Parliament, and Council: Could we please get eIDAS Article 24.1 right with eIDAS 2.0?*" e pubblicata su: https://www.linkedin.com/pulse/dear-eu-commission-parliament-council-could-we-please-jon-%25C3%25B8lnes/?trackingId=6oiTKhh9SIaOM8TbZwd07Q%3D%3D.

[6] "Open Letter from Cloud Signature Consortium and Qualified Trust Services Organizations Warns of Risks in eIDAS 2 Regulation", pubblicata in data 01/02/2023 e sottoscritta dal consorzio internazionale CSC – Cloud Signature Consortium, dall'italiana AssoCertificatori, l'associazione europea ESD – European Signature Dialog, la Spagnola ASPEC – Asociación de Prestadores Cualificados de Servicios de Confianza de España, la francese ClubPSCO – Club des Prestataires de Services de Confiance. La lettera è disponibile (in inglese) al link: https://cloudsignatureconsortium.org/risks-of-eidas-2-art-24-to-eu-citizens-the-trust-service-sector-open-letter/

lioni di cittadini dotati di carta d'identità elettronica in Germania, nel 2021 questi avevano utilizzato la funzione eID solamente 11 milioni di volte, comparandolo con oltre il miliardo di transazioni SPID 2 in Italia.

Nella lettera le associazioni firmatarie sottolineavano inoltre come l'eliminazione della possibilità di ricorrere al LoA significativo potesse in concreto rivelarsi una eterogenesi dei fini: se è chiaro che l'intento del Legislatore fosse quello di innalzare il più possibile il livello di garanzia e di fiducia – anche auspicando la massima diffusione della firma qualificata – al contempo rinunciare a metodi di identificazione facili da usare andrebbe a mettere a rischio questo obiettivo. La lettera offre l'esperienza concreta dei QTSP associati suggerendo che, poichè l'utente cerca sempre la facilità d'uso, rendere più complesso ottenere un certificato qualificato orienti naturalmente la sua scelta su opzioni più *easy-to-use* perché meno regolamentate e con un minore livello di garanzia, quali sono le firme avanzate. Quindi, si sosteneva, con l'intento di aggiungere sicurezza si arriverebbe in realtà a un abbassamento del livello generale di *trust*, almeno fino alla completa e compiuta diffusione del portafoglio di identità digitale, previsto in un orizzone di medio termine. Per questi motivi la richiesta era "*reinstate the assurance level "substantial" in article 24 (in line with the Commission's initial proposal), and revisit the issue in the future, following further assessment of the feasibility of LoA "high*". Questa richiesta, come noto, non è stata accolta: sarà pertanto interessante osservare come i QTSP raccoglieranno la sfida e se davvero questa scelta porterà a una ritirata nell'uso dei certificati qualificati in alcuni casi d'uso dove attualmente sono lo standard di fatto.

Proseguendo nella disamina dei metodi di identificazione ammessi, la lettera b) del comma 2 dell'articolo 24 conferma l'opzione di utilizzare un **certificato qualificato** preesistente per emettere un nuovo certificato qualificato, scelta prevalente nei processi di rinnovo dei certificati. Vi è una novella importante rispetto alla precedente versione del Regolamento: scompare infatti la previsione che il preesistente certificato sia stato emesso previa identificazione in presenza o utilizzando un mezzo di identificazione elettrodica; diventa quindi possibile anche il rinnovo di certificati emessi con procedure di identificazione remota – o comunque rientrante tra le "altre modalità" ammesse previo audit di un CAB – prima teoricamente non possibile.

La lettera c) offre qualche opzione di flessibilità e anche di innovazione in quanto dispone la possibilità per i QTSP di ricorrere a generici "**altri metodi di identificazione**" a patto che il livello di sicurezza dell'identificazione sia elevato e la conformità dei quali sia confermata da un organismo di valutazione della conformità. Nel testo novellato viene espunto il preesistente riferimento alla "garanzia equivalente alla presenza fisica del titolare del certificato": l'identificazione in presenza non è quindi più il metro di misura della sicurezza dell'identificazione. Rimane tuttavia un certo livello di interpretabilità su cosa si indichi con "elevato livello di sicurezza", concetto non definito nel Regolamento (al contrario del "livello di garanzia" o LoA, concetto differente e definito all'articolo 8) e che potrebbe trovare mitigazione grazie all'emissione dell'atto di esecuzione previsto dal novellato articolo 24, al comma 1-quater.

Infine, l'ultima modalità di identificazione ammessa (lettera d)) è la "**presenza concreta** *della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale*". Scompare nella versione definitiva, rispetto alla proposta iniziale della Commissione, l'opzione "se non sono disponibili altri mezzi" riportando il riconoscimento in presenza con pari dignità rispetto alle altre modalità e, come abbiamo già avuto modo di commentare, viene espressamente previsto un riferimento al diritto nazionale per regolare opportune specificità locali.

In aggiunta ai quattro metodi tipizzati, il QTSP avrà l'opzione di verificare l'identità anche mediante una loro **combinazione**: è una innovazione rispetto alla versione precedente del Regolamento e alla proposta della Commissione che apre a una serie di domande. In primis, che cosa si intende con "combinazione"? Non è un concetto definito, che probabilmente non è una semplice "somma" di diverse modalità di identificazione. Ricade questa, per caso, nella modalità dettagliata alla lettera c), che quindi va progettata in anticipo e quindi sottoposta alla verifica di un CAB per la emissione di un CAR che ne attesti la conformità? Se così fosse, il suo inserimento al comma 1-bis potrebbe essere considerato pleonastico. Oppure è da considerarsi invece categoria residuale, qualora l'uso di una singola modalità tipizzata non assolva pienamente allo scopo, e quindi serva un rafforzativo dei dati raccolti? Si auspica che la Commissione Europea faccia luce su questi dubbi, mediante gli atti di esecuzione previsti.

4. La verifica degli attributi

Il comma 1 ter dell'articolo 24 regolamenta le modalità di verifica degli attributi in un processo di emissione di una attestazione elettronica di attributi qualificati:

> *1 ter. La verifica degli attributi di cui al paragrafo 1 è effettuata, con mezzi adeguati, dal prestatore di servizi fiduciari qualificato, direttamente o tramite un terzo, sulla base di uno dei metodi seguenti o una combinazione degli stessi, ove necessario, conformemente agli atti di esecuzione di cui al paragrafo 1 quater:*
>
> *a) mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato;*
>
> *b) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato in conformità del paragrafo 1 bis, lettera a), c) o d);*
>
> *c) mediante un attestato elettronico di attributi qualificato;*
>
> *d) mediante altri metodi che garantiscono la verifica degli attributi con un elevato livello di sicurezza, la conformità dei quali è confermata da un organismo di valutazione della conformità;*

e) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale.";

La struttura del comma 1-ter è congruente con quanto esposto sopra per i certificati qualificati: ritroviamo infatti il concetto di verifica degli attributi con mezzi adeguati, la tipizzazione dei metodi e l'apertura alla possibilità di combinarli, nonché la necessità di essere conformi agli emanandi atti di esecuzione.

Anche per gli attributi, il livello di garanzia richiesto per l'uso del por**tafoglio europeo di identità digitale** o di un **mezzo di identificazione elettronica** è elevato, così come è possibile l'utilizzo di **certificati qualificati** per firma elettronica e sigillo (attenzione, non si citano i certificati qualificati di autenticazione dei siti web).

Una opzione aggiuntiva è quella dell'uso di un preesistente **attestato elettronico di attributi qualificato** per eseguire le verifiche necessarie per il rilascio di un nuovo attestato, previsione che va in coerenza con l'articolo 45-ter sugli effetti giuridici degli stessi[7]. Non viene tuttavia citata la possibilità di avvalersi, per fini di verifica prima dell'emissione, di attestati di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica nonostante questi siano equipollenti agli attestati qualificati: si ritiene che, proprio in virtù dell'equipollenza, essi siano utilizzabili ma si auspica in ogni caso che venga chiarito in sede di atto di esecuzione, per fugare ogni possibile dubbio.

Le ultime due modalità di verifica riferiscono alla **presenza concreta** del titolare e a non meglio specificate "**altre modalità**" confermate da un CAR e in conformità con un atto di esecuzione.

Anche per le verifiche connesse all'emissione di attributi, pertanto, la normativa di esecuzione diventa fondamentale; come vedremo nel paragrafo successivo, su questo tema la complessità dell'attività che la Commissione Europea deve portare avanti è rilevante, con la sfida di mantenere la coerenza tra tutti gli elementi.

---

[7] Articolo 45 ter
Effetti giuridici degli attestati elettronici di attributi

1. A un attestato elettronico di attributi non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per gli attestati elettronici qualificati di attributi.
2. Un attestato elettronico di attributi qualificato e gli attestati di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto hanno gli stessi effetti giuridici degli attestati in formato cartaceo rilasciati legalmente.
3. Un attestato di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica in uno Stato membro, o per suo conto, è riconosciuto come un attestato di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto in tutti gli Stati membri.

5. Gli atti di esecuzione e le misure transitorie

Come spesso richiamato in questa disamina, gli atti di esecuzione sono l'elemento fondamentale per l'implementazione operativa delle modalità di verifica dell'identità e degli attributi dettate dall'articolo 24. Il comma 1-quater recita infatti:

> *1 quater. Entro 12 mesi dalla data di entrata in vigore del presente regolamento modificativo la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure per la verifica dell'identità e degli attributi conformemente ai paragrafi 1, 1 bis e 1 ter. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.*

Lo standard che si candida a essere referenziato dagli atti di esecuzione per i processi di verifica dell'identità è certamente la *technical specification* ETSI TS 119 461 V1.1.1[8], emessa nel luglio 2021 dall'ente di standardizzazione ETSI: frutto di un intenso lavoro di razionalizzazione, la norma stabilisce i requisiti di sicurezza e politica per i componenti dei servizi fiduciari che forniscono la verifica dell'identità dei soggetti, sia quando questi sono direttamente forniti dal TSP come parte integrante del servizio, sia quando essi siano erogati da un Fornitore di Servizi di Verifica dell'Identità (*IPSP – Identity Proofing Service Provider*) specializzato, che quindi agisce come subappaltatore per il TSP. La norma fornisce pertanto requisiti per un Livello Base di Verifica dell'Identità (*LoIP – Level of Identity Proofing*) volto a supportare soprattutto l'emissione di certificati qualificati come definito nell'articolo 24.1 del Regolamento (UE) n. 910/2014.

Con il Regolamento in modifica e a fronte di un contesto tecnologico e di mercato profondamente mutato, ETSI ha ritenuto necessario avviare una attività di revisione e aggiornamento di tale norma[9], anche con lo scopo di allineare la TS 119 461 ai requisiti del nuovo quadro di Identità Digitale recato dal portafoglio EUDI. Al momento di scrittura di questo articolo, i lavori del gruppo di revisione non sono ancora conclusi: tra gli obiettivi vi è quello di aggiornare i requisiti e i casi d'uso per riflettere i nuovi requisiti di verifica dell'identità recati dall'articolo 24, includendo nella norma anche indicazioni e requisiti per verifica dell'identità per l'emissione di attestazioni di attributi elettronici e per l'uso di queste nei processi di verifica dell'i-

---

[8] "Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects" disponibile su https://www.etsi.org/deliver/etsi_ts/119400_119499/119461/01.01.01_60/ts_119461v010101p.pdf

[9] Si veda in particolare la pagina dedicata nel portale ETSI al seguente link: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=68548&curItemNr=14&totalNrItems=28&optDisplay=100000&qSORT=REFNB&qETSI_ALL=&SearchPage=TRUE&qTB_ID=607%3BESI&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qEND_CURRENT_STATUS_CODE=11+WI%3BM58&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qFREQUENCIES_BOOLEAN=OR&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY

dentità[10].

ETSI 119 461, nella versione rivista, si candida pertanto ad essere la *baseline* di partenza per gli atti di esecuzione sia per quanto riguarda la verifica dell'identità, sia per quanto riguarda la verifica degli attributi.

Per questi ultimi, lo scenario presenta una notevole complessità, in quanto il Regolamento dispone che la Commissione Europea emani:

- uno o più atti ai sensi dell'articolo 24 comma 1-quater, che dovranno recare norme di riferimento, stabilire specifiche e procedure per la verifica dell'identità e degli attributi, entro 12 mesi dall'entrata in vigore del Regolamento modificativo;
- uno o più atti ai sensi dell'articolo 45-quinquies comma 5, che dovranno contenere un elenco di norme di riferimento e, se necessario, specifiche e procedure applicabili agli attestati elettronici qualificati di attributi, entro 6 mesi dall'entrata in vigore del Regolamento modificativo;
- uno o più atti ai sensi dell'articolo 45-sexies comma 2, che dovranno definire un elenco di norme di riferimento e, se necessario, specifiche e procedure per le procedure di verifica degli attestati elettronici qualificati di attributi rispetto alle fonti autentiche, entro 6 mesi dall'entrata in vigore del Regolamento modificativo;
- uno o più atti ai sensi dell'articolo 45-septies, recanti norme, procedure e indicazioni per l'emissione degli attestati di attributi direttamente da parte di un organismo del settore pubblico responsabile di una fonte autentica, entro 6 mesi dall'entrata in vigore del Regolamento modificativo.

Si tratta quindi di un complesso sistema di norme tecniche, procedure, atti di esecuzione che dovranno essere mantenuti in coerenza tra loro, pena l'emergere di aree di incertezza che possono minare l'affidabilità stessa delle procedure di verifica.

La stessa necessità di coerenza e organicità si riscontra su di un punto molto specifico, che tuttavia potrebbe essere di grande interesse per i QTSP italiani. Si tratta di quanto previsto dall'articolo 5-bis al comma 24:

> *La Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure per facilitare l'onboarding degli utenti nel portafoglio europeo di identità digitale tramite mezzi di identificazione elettronica conformi al livello di garanzia elevato o mezzi di identificazione elettronica conformi al livello di garanzia significativo unitamente a ulteriori procedure di onboarding a distanza che, insieme, soddisfano i requisiti del livello di garanzia elevato. Tali atti di esecuzione sono adottati*

[10] Tra gli obiettivi del gruppo di lavoro di revisione della norma vi è anche quello di fornire uno standard adatto come base per la parte di verifica dell'identità dell'onboarding PID al Portafoglio EUDI, in coordinamento con il CEN/TC 224, ovvero il comitato tecnico del Comitato Europeo di Normazione (CEN) che sviluppa standard per rafforzare l'interoperabilità e la sicurezza dell'identificazione personale e dei dispositivi personali correlati.

secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Nella pletora di atti di esecuzione relativi al portafoglio europeo di identità digitale, pertanto, ve ne sarà uno specifico per l'identificazione, che specificherà processi di "combinazione" tra un mezzo di identificazione elettronica con LoA significativo e altre procedure di onboarding a distanza, che saranno adatte all'inizializzazione del portafoglio stesso. Ora, se il livello di garanzia previsto per il portafoglio è elevato, ragionando per analogia queste "combinazioni" dovrebbero essere adatte anche all'identificazione ex articolo 24. Si auspica pertanto che questi due filoni di normativa secondaria siano mantenuti allineati, così da garantire coerenza sistemica e non disperdere il patrimonio di esperienza costruito con l'esperienza SPID.

Si ritiene utile sottolineare un ulteriore elemento: il Regolamento non dispone il divieto per gli Stati Membri di introdurre ulteriori requisiti e specifiche gravanti sui QTSP vigilati, né presenta specifiche disposizioni transitorie miranti a ricondurre a quanto disposto dagli atti di esecuzione, le numerose normative nazionali che ora regolamentano la verifica dell'identità. Non è escluso pertanto che normative nazionali come la francese PVID[11], il registro dei prestatori di servizi di identificazione presente in Romania[12], le normative di certificazione previste dal regolatore spagnolo[13], rimangano operative e gravanti sui prestatori vigilati nel Paese. Questo implicherebbe un ostacolo rilevante sulla strada di quell'armonizzazione di approcci, standard, livelli di sicurezza auspicata dal Legislatore Europeo, nonché costi aggiuntivi per i QTSP.

Una chiosa, infine, sulle misure transitorie previste all'articolo 51, comma 4:

4. I prestatori di servizi fiduciari qualificati cui è stata assegnata la qualifica a norma del presente regolamento prima del ... [data di entrata in vigore del presente regolamento modificativo] *presentano all'organismo di vigilanza una relazione di valutazione della conformità che attesti il rispetto dell'articolo 24, paragrafi 1, 1 bis e 1 ter, quanto prima e comunque entro il ...* [24 mesi dall'entrata in vigore del presente regolamento modificativo].

I QTSP hanno pertanto 24 mesi di tempo dall'entrata in vigore del Regolamento novellato per dimostrare all'Autorità di Vigilanza il rispetto pieno delle nuove modalità di identificazione recate. Sorge tuttavia un dubbio sulle modalità ammesse

---

[11] La normativa PVID – Prestataire de Verification d'Identité à Distance, è la normativa emanata dall'autorità di vigilanza ANSSI, recante i requisiti e i processi di accreditamento per la verifica di identità a distanza in Francia. Info su: https://cyber.gouv.fr/prestataires-de-verification-didentite-distance-pvid

[12] La lista dei soggetti autorizzati è pubblicata dall'autorità di vigilanza della Romania ADR: https://www.adr.gov.ro/identificare-la-distanta-prin-mijloace-video/

[13] Si tratta dell'"Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados", pubblicato sul Bollettino Ufficiale di Spagna (BOE) numero 115, del 14 maggio 2021(https://www.boe.es/eli/es/o/2021/05/06/etd465).

nel periodo transitorio: il QTSP rimane autorizzato a continuare a identificare secondo quanto autorizzato in precedenza, almeno fino alla conclusione del processo di notifica del nuovo rapporto di conformità? Oppure, adottando una interpretazione restrittiva, dal momento di entrata in vigore della nuova versione di eIDAS deve cessare l'uso di tutte le modalità di identificazione difformi dal novellato articolo 24, come ad esempio i mezzi di identificazione elettronica notificati di livello significativo qual è SPID 2?

Una delle proposte intermedie di compromesso, poi modificata in corso d'opera, autorizzava espressamente i QTSP a continuare ad avvalersi di quanto in essere fino alla presentazione della relazione di valutazione della conformità: il fatto che di questo non si rilevi traccia nel testo finale lascia un'area di potenziale interpretazione che potrebbe portare a posizioni difformi tra le diverse autorità degli Stati Membri o, ancor peggio, tra diversi attori di mercato. Si auspica pertanto che l'Autorità di Vigilanza o la Commissione, anche solo in una FAQ pubblicata sul proprio sito[14], dirima la questione.

6. Gli impatti sul mercato dei QTSP: alcune previsioni

Approcciando la conclusione di questo scritto, non possiamo esimerci da una valutazione degli impatti di quanto analizzato. Come sottolineato in apertura, l'articolo 24 è uno di quelli che impatta profondamente sulla struttura dei costi e la competitività di un QTSP che emette certificati qualificati e, in futuro, su quelli che emetteranno attestati elettronici di attributi qualificati.

In un mercato dove l'attrattività commerciale è direttamente influenzata dalla *user experience*, ogni vincolo in più al processo diventa una sfida per rimanere competitivi.

La scelta di innalzare il livello di garanzia a elevato implicherà, per i QTSP italiani, di abbandonare l'uso dell'identità digitale SPID di livello 2 nei processi di identificazione; questo avrà due ordini di conseguenze: una per il QTSP che si troverà un processo più costoso e complesso, l'altra per il Gestore di Identità Digitale che vedrà diminuire i corrispettivi da utilizzo di SPID da soggetti privati, rendendo ancora meno sostenibile tutto il sistema. Potenzialmente la diffusione di SPID di livello 3 potrebbe essere la soluzione, anche se non risolutiva in assenza di una chiara indicazione della sua necessità anche l'accesso a altri servizi pubblici, che ne aiuterebbe la diffusione.

I QTSP, nel medio termine, potranno inoltre certamente beneficiare di una maggiore diffusione della CIE, dell'IT-Wallet[15] e, quando disponibile, del portafoglio

[14] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ

[15] L'IT-Wallet, è una iniziativa del Governo Italiano introdotta dal decreto 26 febbraio PNRR, è una iniziativa di portafoglio digitale che consente di conservare documenti digitali all'interno dell'app

europeo di identità digitale: si tratta tuttavia di sistemi che al momento non hanno la diffusione o la maturità tale a sostenere le necessità dei processi di emissione di certificati digitali; l'effetto della norma è quindi quello di eliminare una opzione, lo SPID 2, senza che altre altrettanto diffuse siano disponibili.

Questa dinamica comporterà quindi la necessità per il QTSP di individuare altre modalità di identificazione, soprattutto da remoto, con una prevalenza di riconoscimenti in modalità self-service, principalmente di tipo *unattended* o *hybrid-unattended* con la presenza di un controllo di back-office, regolamentati dalla ETSI TS 119 461 (nell'ipotesi che questo standard diventi il cuore dell'atto di esecuzione). È quindi prevedibile che i costi dei processi di riconoscimento si innalzeranno, mettendo i Certificatori di fronte alla scelta di aumentare i listini o vedere i propri margini compressi.

In alcune situazioni, inoltre, non è remota la possibilità che lo scenario dipinto dalla lettera aperta di CSC si realizzi: i processi di emissione di certificati qualificati di firma, molto spesso, sono integrati in altri processi di business, come quelli di apertura di conti correnti, firma di contratti di finanziamento, selezione di dipendenti. La necessità di cambiare questi processi potrebbe portare i clienti a rivalutare il ruolo stesso del certificato qualificato di firma, optando per altre soluzioni come ad esempio la firma avanzata, almeno nel breve termine. Nel medio termine, invece, se e quando il portafoglio di identità digitale e gli attestati di attributo saranno di uso comune, la loro diffusione potrebbe giustificare gli investimenti in riprogettazione e integrazione dei sistemi, e la connessa ripresa di appeal dell'uso del certificato qualificato.

In generale, comunque, il restringimento delle opzioni per il riconoscimento comporterà ai QTSP maggiori costi, la necessità di ripensare alle modalità di gestione della loro rete di Autorità di Registrazione (anche il riconoscimento in presenza sarà regolamentato dall'atto di esecuzione), minori leve di differenziazione della *user experience*. Sarà uno sviluppo interessante da osservare, che potrebbe cambiare anche i rapporti di forza nel mercato, in presenza di innovazioni rilevanti.

IO. In prospettiva, le attese sono di una convergenza tecnologica, funzionale e di governance tra IT-Wallet e EUDI Wallet.

Rivista elettronica di Diritto, Economia, Management
N. 4 - 2024 - pp. 223-234

Il recapito elettronico: scenari ed evoluzione tecnologica dei servizi alla luce degli aggiornamenti normativi in Italia e in Europa

Flavio Fanton - Enrico Giunta - Federica Marti

Abstract [IT]: Normativa e contesti d'uso hanno portato, nel quadro italiano, alla preminenza della Posta Elettronica Certificata quale strumento tecnologico di recapito elettronico. Il Regolamento eIDAS ha rappresentato un'occasione di apertura verso altre forme di recapito elettronico: solo recentemente il panorama normativo italiano sta recependo le potenzialità prospettate a livello europeo, parallelamente allo sviluppo delle iniziative che porteranno al passaggio dalla PEC alla REM. Il nuovo regolamento 2024/1183 (nel seguito eIDAS 2.0) si focalizza sul tema dell'interoperabilità tra le soluzioni di recapito elettronico e sul mutuo riconoscimento dei Paesi membri di queste ultime, determinando, anche a livello nazionale, la necessità di estendere le riflessioni in quest'ambito. Il presente contributo si propone di presentare un'analisi del contesto corrente sul tema, finalizzata alla disamina delle prospettive e delle potenzialità sul mercato italiano ed europeo per i soggetti che erogano tali soluzioni.

Abstract [EN]: Regulatory framework and contexts of use have led, in the Italian framework, to the very preponderance of PEC (Posta Elettronica Certificata - Certified Electronic Mail) as a technological tool for electronic delivery. The eIDAS Regulation has represented an opportunity to open up to other forms of electronic delivery: only recently has the Italian legislative landscape been incorporating the potential prospected at the European level, in parallel with the development of the initiatives that will lead to the transition from PEC to REM (Registered Electronic Mail). The new regulation 2024/1183 (eIDAS 2.0 in the following text) focuses on the issue of interoperability between electronic delivery solutions and the mutual recognition of EU member countries, determining, also at the national level, the need to extend the considerations in this area. The aim of this contribution is to present an analysis of the current context on the subject, intended to examine the prospects and potential in the Italian and European markets for entities providing such solutions.

1. Introduzione

eIDAS 2.0[1] costituisce la nuova versione del Regolamento n. 910/2014[2], comunemente noto come eIDAS (*Electronic Identification And trust Services*), riguardante l'identificazione elettronica e i servizi per le transazioni elettroniche nel mercato interno europeo. Il nuovo Regolamento espande il panorama dei *qualified trust services*, introducendone di nuovi e aprendo ulteriori prospettive per quelli già in esso inclusi.

Tra gli strumenti già normati dal Regolamento, sin dalla sua prima versione, vi è il recapito elettronico: questo è definito, nell'articolo 3, come un «servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate» (*Electronic Registered Delivery Service* – ERDS). Questo, nella sua versione qualificata (*Qualified Electronic Registered Delivery Service* – QERDS) è descritto come un «servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44»[3].

In Italia, tuttavia, nell'ambito dei servizi di recapito elettronico è preponderante l'utilizzo della Posta Elettronica Certificata (PEC), mezzo di comunicazione preesistente ad eIDAS. Tale strumento consiste in un «sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi», come delineato dal comma 1, lettera v-bis) del D.lgs. 7 marzo 2005, n.82 *Codice dell'Amministrazione Digitale*[4].

Con l'avvento di eIDAS, si è avviato il percorso che dalla PEC vedrà la transizione alla REM (*Registered Electronic Email*), anche nota come PEC europea: questo mezzo di recapito si caratterizza per la piena conformità con i requisiti del Regolamento 910/2014 e per l'impiego della REM *Baseline*, ovvero «l'insieme minimo di requisiti che mirano a garantire la massima interoperabilità nel settore dell'interoperabilità cross-REM e, in particolare, nell'uso transfrontaliero dei servizi REM»[5].

---

[1] *Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.* Le citazioni degli articoli del testo di eIDAS 2.0 sono esplicitate nel prosieguo dell'articolo in lingua inglese.

[2] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.* Le citazioni degli articoli del Regolamento eIDAS, nel prosieguo del testo, saranno esplicitate in lingua italiana.

[3] È scelta autoriale utilizzare i termini ERDS e QERDS nel prosieguo dell'articolo, in luogo delle versioni italiane SERC (Servizio Elettronico di Recapito Certificato) e SERCQ (Servizio Elettronico di Recapito Certificato Qualificato).

[4] Da ora in avanti CAD.

[5] Si veda il documento *REM SERVICES – Criteri di adozione standard ETSI – Policy IT*, Agenzia per l'Italia Digitale, Versione 1.2, pubblicato al link <https://www.agid.gov.it/sites/default/files/repository_files/documento_finale_gdl_rem_versione_1.2_28.07.2022_1.pdf> (ultima consultazione: 20/04/2024).

2. Il recapito elettronico Italia: la PEC e gli impatti del primo regolamento eIDAS

L'Italia si distingue per l'aver sviluppato, a partire dal 2005, e reso di uso comune un mezzo di recapito elettronico antecedente a eIDAS, ovvero la Posta Elettronica Certificata.

L'entrata in vigore del Regolamento 910/2014 ha dato luogo a due effetti apparentemente contrastanti.

Da un lato, vista la rilevanza che la normativa nazionale ha conferito alla PEC e l'ampio utilizzo che ne ha conseguito da parte delle Pubbliche amministrazioni, delle aziende, degli ordini e dei professionisti, non si è verificata la necessità di forti adeguamenti normativi né si sono generate dinamiche di mercato che spingessero la creazione di nuove tipologie di recapito elettronico.

Dall'altro, l'introduzione del regolamento eIDAS ha rappresentato un momento significativo nello scenario della comunicazione elettronica a valore legale in Italia: ha permesso di mettere in discussione il servizio PEC, affrontando alcune carenze emerse nel tempo, e di avviare il percorso verso la REM, con lo scopo di aumentare gli standard di sicurezza e, soprattutto, compiendo un passo significativo verso l'adozione di uno standard europeo che promuove l'interoperabilità transfrontaliera.

Quanto al primo scenario, le modifiche al quadro normativo che hanno dovuto avere luogo sono state condizionate, nello specifico, dagli articoli 43 e 44 del Regolamento.

L'articolo 43, in primo luogo, si sofferma sugli effetti giuridici di un servizio elettronico di recapito certificato:

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.

Le garanzie aggiuntive del recapito qualificato sono da riferirsi ai requisiti fissati dall'articolo 44, ovvero:

1. I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:
   a. sono forniti da uno o più prestatori di servizi fiduciari qualificati;
   b. garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c. garantiscono l'identificazione del destinatario prima della trasmissione dei dati;
d. l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;
e. qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
f. la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Il principale provvedimento italiano che ha dovuto recepire tali input è costituito dal CAD, in quanto, tra gli altri aspetti, questo disciplina le modalità di trasmissione delle comunicazioni elettroniche.

L'art. 1, comma 1, lett. n-ter) del CAD definisce, in particolare:

> n-ter) domicilio digitale: un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Regolamento eIDAS", valido ai fini delle comunicazioni elettroniche aventi valore legale"

> Inoltre, sempre l'art.1, comma 1-ter, del CAD, prevede che:
> Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.

Di fatto, quindi, il legislatore italiano ha parificato il valore legale dei recapiti qualificati a norma eIDAS alla Posta Elettronica Certificata. Solo in tempi recenti, però, con l'approdo in Italia di mezzi di recapito diversi dalla PEC, si è iniziato a operare una riflessione in merito a quanto espresso negli articoli indicati.

È evidente, infatti, che tale parificazione risulti "sproporzionata" e consista in una forzatura a vantaggio della PEC. Quest'ultima, infatti, possiede solamente le caratteristiche di un ERDS e non di un QERDS, mancando del fondamentale passaggio di identificazione certa a norma eIDAS dei soggetti coinvolti nel processo di comunicazione[6]. Tale modifica al CAD, pertanto, può essere vista – adottando un punto di

[6] Il riferimento è ai mezzi di identificazione previsti dall'articolo 24 del Regolamento eIDAS e alle misure previste dal 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*

vista interpretativo – come un tentativo di adeguamento e di apertura del legislatore italiano verso strumenti di recapito più sicuri e imputabili[7].

Come già accennato, è soltanto di recente che a questi principi si sono affiancati dei provvedimenti specifici sui QERDS: è da citare, a tal proposito, il comunicato ARERA del 14/06/2023[8] il quale ha aperto la strada all'utilizzo concreto di tali soluzioni. In tale provvedimento, infatti, si consente agli operatori del settore energetico di sostituire con una comunicazione elettronica qualificata la tradizionale modalità di invio di una raccomandata A/R o PEC relativa alla messa in mora dell'utenza. Tale presa di posizione segue quanto indicato dal CAD, in quanto viene esplicitamente affermato che per tali comunicazioni è necessario un QERDS e che non è sufficiente un ERDS.

Il fatto che i primi servizi di recapito qualificato introdotti in Italia non siano stati sviluppati in ambito nazionale ha spinto altresì la riflessione in merito al mutuo riconoscimento delle soluzioni di recapito all'interno del perimetro comunitario europeo, anche alla luce di un quadro incerto sulle modalità di qualifica presso AgID di tali strumenti e vista la preponderanza della PEC. eIDAS si basa, come noto, su un principio di neutralità tecnologica e sul mutuo riconoscimento dei servizi in esso regolamentati da parte degli Stati membri, indipendentemente dalla nazione entro la quale è stato espletato l'iter di qualificazione, dal momento che in ognuna di esse è designato un apposito *Supervisory Body* incaricato di vigilare su tali servizi. Tali premesse rendono implicita la validità sul territorio europeo della qualifica conseguita in altri Stati comunitari da parte di *provider* di recapito in essi operanti a condizione che siano inseriti nell'apposita *Trusted List* europea[9], la quale include tutti i servizi che - per essere qualificati ai sensi eIDAS - siano stati sottoposti al processo di certificazione dei requisiti dell'art. 24 del Regolamento e, in particolare per i recapiti elettronici qualificati, rispondenti a quelli stabiliti dall'articolo 44.

Quanto agli standard ETSI impiegati, i riferimenti dei *Conformity Assessment Bodies* accreditati per il rilascio della suddetta certificazione sono ETSI EN 319 401: *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trusted Service Providers* e ETSI EN 319 521: *Electronic Signatures and Infrastructures (ESI); Policy and security requi-rements for Electronic Registered Delivery Service Providers*.

Ovviamente si tratta degli stessi standard che – adottati a livello europeo e

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.

[7] Dello stesso parere è l'avvocato Eugenio Prosperetti, consultato dagli autori per la redazione del presente contributo.

[8] Comunicato ARERA del 14 giugno 2023, *Modalità di comunicazione per la costituzione in mora del cliente finale: equiparazione SERCQ, raccomandata AR e PEC – ARERA*, pubblicato al link <https://www.arera.it/comunicati-operatore/dettaglio/it/comunicati/23/230614c> (ultima consultazione: 20/04/2024).

[9] L'elenco di fiducia è consultabile pubblicamente al link <https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home> (ultima consultazione 20/04/2024).

dalla stessa AgID - costituiscono la base anche per l'implementazione della REM in Italia, cui si aggiunge anche ETSI EN 319 532 *Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services*.

Quanto alle specifiche regole tecniche e alle garanzie accessorie, queste sono stabilite da ciascun *Supervisory Body* nazionale, ma non costituiscono una restrizione per l'utilizzo dei servizi nei diversi Paesi comunitari né implicano richieste autorizzative ulteriori.

Ciò considerato, dunque, si ribadisce come il già citato Codice dell'Amministrazione Digitale stabilisca che ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altri servizi di recapito qualificato ai sensi eIDAS e dichiari elegibile come domicilio digitale (oltre alla PEC) un indirizzo elettronico attivato presso un servizio di recapito qualificato eIDAS, il quale domicilio è valido ai fini delle comunicazioni elettroniche aventi valore legale. Si ricorda, a questo proposito, che la PEC non costituisce un servizio costruito sullo schema eIDAS, ma si basa sul Decreto Ministeriale del 2 novembre 2005 *recante le Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*: la normativa in Italia equipara questa tipologia di recapito a un QERDS per esigenze proprie ma, dal punto di vista degli elementi probatori che quest'ultimo fornisce, risultano delle aggiunte non trascurabili.

I vincoli normativi su cui si basa la PEC, infatti, non contemplano l'identificazione certa del titolare della casella, condizione, invece, imprescindibile per un QERDS.

Si riprende, dunque, il secondo punto di riflessione iniziale, ovvero l'impatto del Regolamento eIDAS sul principio del percorso di transizione dalla PEC alla REM.

Grazie alla sua consolidata esperienza, l'Italia avrebbe potuto limitarsi a minori aggiustamenti della PEC per soddisfare i criteri dei servizi di recapito qualificato. Tuttavia, ha optato per lo standard ETSI REM, una scelta ambiziosa che mira a un modello di interoperabilità su larga scala. Questa transizione ha richiesto un impegno considerevole da parte degli attori coinvolti, non solo sul piano tecnico ma anche in termini organizzativi e commerciali, consolidando il numero di Gestori PEC e introducendo nuovi rischi su un servizio tecnicamente e giuridicamente stabile da anni.

Un elemento cruciale in questo senso è stato il rafforzamento del livello minimo di garanzia dell'identità dei titolari della casella di posta elettronica. La normativa vigente lo ha definito nelle *Linee guida per la vigilanza sui gestori di posta elettronica certificata*[10], al capitolo. 8.1 *Servizio di Registrazione dei titolari*: «il Gestore verifica in modo affidabile l'identità dei titolari all'atto della registrazione e ne conserva i dati in modo sicuro». La modalità di verifica dell'identità del titolare cosiddetta affidabile è declinata da ciascun Gestore all'interno del proprio manuale operativo, ma il livello minimo di sicurezza di tale processo è stato oggetto di

[10] *Linee guida CNIPA per la vigilanza sui gestori di posta elettronica certificata (Art. 14 comma 13 Decreto Presidente della Repubblica 11 FEBBRAIO 2005, N. 68)* V 1.0 18 novembre 2009.

dibattito per lungo tempo fino a raggiungere un compromesso. Questo periodo di discrezionalità ha reso complessa l'analisi dei processi e l'elaborazione di soluzioni adeguate da parte dei Gestori, ma, allo stesso tempo, ha fornito a coloro che hanno interpretato i dettami in maniera meno restrittiva, sensibili opportunità di business.

Va ricordato, in questo contesto, che scopo della PEC è garantire, tra l'altro, la provenienza, l'integrità e l'autenticità del messaggio[11]. In particolare, provenienza e autenticità si intendono garantite dal Gestore: questo perché gli avvisi, le ricevute, ma soprattutto le buste di trasporto sono firmate con firma elettronica avanzata rilasciata al Gestore stesso, la quale assicura l'associazione del messaggio con il soggetto titolare limitatamente ai processi di verifica dell'identità definiti nel manuale operativo del singolo fornitore.

La consapevolezza di dover colmare tale lacuna relativa al requisito di autenticità ha portato, in passato, alla definizione, nel DPCM 27 settembre 2012, di una modalità di identificazione maggiormente adeguata al rilascio di una casella PEC ai fini della presentazione, in via telematica, di istanze e dichiarazioni alle Pubbliche amministrazioni[12]. La soluzione, definita PEC-ID, prevedeva che il soggetto titolare della casella venisse identificato in modo certo e che l'accesso al servizio fosse mediato da un meccanismo di autenticazione forte.

Gli articoli 5 e 6 del suddetto decreto precisano le condizioni di tali passaggi:

Art. 5 - Modalità di identificazione dei Titolari di caselle PEC-ID

1. Le operazioni di identificazione del Titolare sono curate dal Gestore nell'ambito delle attività e delle funzioni per la registrazione di cui all'art. 21, comma 1, lettera a) del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005.
2. L'identificazione di cui all'art. 65, comma 1, lettera c-bis) del CAD avviene, in occasione di ogni attribuzione di credenziali di accesso, in uno dei seguenti modi:
   a. mediante la sottoscrizione del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD ed esibizione al Gestore, da parte del Titolare, di un valido documento d'identita' e del codice fiscale;
   b. tramite la compilazione del modulo di adesione disponibile in rete, previa identificazione informatica tramite CIE o CNS;
   c. mediante la sottoscrizione con firma digitale, di cui all'art. 1, comma 1,

[11] Come previsto dall'art.9, comma 2 del Decreto del Presidente della Repubblica 11 febbraio 2005, n.68
Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.

[12] Decreto del Presidente del Consiglio dei Ministri 27 settembre 2012 *Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo 65, comma 1, lettera c-bis), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni.*

lettera s) del CAD, del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD;

   d. a mezzo di apparecchiature che utilizzino necessariamente una SIM/USIM dotate di codici PIN/PUK o loro evoluzioni tecnologiche rilasciate previa identificazione del titolare delle medesime nel rispetto delle disposizioni vigenti.

3. Il Gestore verifica la corrispondenza dei dati forniti dal Titolare con le generalita' indicate nel documento d'identita' o associate alla SIM/USIM e conserva la relativa documentazione per il periodo di durata del servizio PEC-ID e per un periodo pari a ventiquattro mesi successivi alla cessazione del servizio PEC_ID.
4. Nel modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD il Titolare manifesta l'eventuale assenso di cui all'art. 6 del CAD.

Art. 6 - Identificazione

1. Ai fini dell'identificazione per l'accesso al servizio PEC-ID, il Gestore predispone una delle seguenti modalita':
   a. identificazione tramite Certificato di autenticazione della CNS;
   b. identificazione tramite Certificato di autenticazione della CIE;
   c. identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) trasmessa attraverso sistemi di telefonia mobile;
   d. identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) generata dal token crittografico rilasciato dal Gestore medesimo.

L'iniziativa non ha avuto particolare successo, ma ha sicuramente segnato una tappa importante nel percorso di affermazione della necessità di identificazione certa dei titolari, che ha visto il suo compimento con l'entrata in vigore del Regolamento eIDAS.

Un ulteriore elemento di complessità, sia dal punto di vista dell'identificazione sia da quello dell'autenticazione multi fattore, è rappresentato dalla pratica diffusa tra i titolari di caselle PEC di condividere le credenziali di accesso tra più persone: basti pensare alle PEC che fanno capo al reparto di un'azienda o ad un'area della Pubblica amministrazione, a quelle comunicate al Registro Imprese, oppure al caso del professionista che delega l'utilizzo della casella al proprio commercialista o segretario per suo conto. Per ovviare a tali problematiche i Gestori hanno messo a disposizione, nel corso del tempo, soluzioni specifiche di accesso multiutente per consentire a terzi l'utilizzo della casella.

3. Le esperienze applicative di recapito elettronico qualificato

Gli strumenti di recapito elettronico qualificato si caratterizzano per la pluralità di soluzioni implementabili allo scopo di trasmettere comunicazioni in forma digitale con la garanzia di identificazione certa di destinatario e mittente e di avvenuti invio e consegna.

In Europa sono attivi quarantasette *Qualified Trust Service Providers* che erogano servizi di recapito elettronico qualificato, ciascuno con la propria soluzione tecnologica. Tali fornitori risultano collocati in Belgio, Bulgaria, Germania, Spagna, Francia, Slovacchia, Ungheria, Italia, Lussemburgo, Olanda, Polonia e Slovenia[13].

A livello implementativo, le modalità di identificazione che risultano impiegate coprono tutto lo spettro di possibilità offerto dal Regolamento eIDAS. Quanto alle opzioni 'de visu', il riconoscimento del mittente e del destinatario è espletabile mediante la presenza concreta della persona fisica presso gli uffici del fornitore o dei rispettivi distributori (*Local Registration Authorities*). Relativamente agli scenari 'a distanza', sono utilizzabili mezzi di identificazione elettronica che sottintendono la previa garanzia della presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica (ad esempio, in contesto italiano, SPID e CIE), certificati di una firma elettronica qualificata o di sigillo elettronico qualificato o altri metodi di identificazione – debitamente verificati, valutati e autorizzati – che forniscono una garanzia equivalente sotto il profilo dell'affidabilità (ad esempio, soluzioni di *onboarding* automatizzato e video riconoscimento).

Quanto al mezzo di comunicazione stesso, vi sono diverse alternative. Il canale e-mail costituisce una delle opzioni principali: il mittente, interagendo con la piattaforma del fornitore e avendo già raccolto il contatto del destinatario, invia a quest'ultimo una e-mail quale vettore del contenuto della comunicazione stessa, che potrà essere fruito solo previa identificazione.

Altri provider mettono a disposizione modalità di trasmissione che impiegano la messaggistica integrata nella telefonia mobile (SMS) o quella di applicazioni proprietarie (Whatsapp) per veicolare la comunicazione: anche in questi casi il destinatario potrà accedere al contenuto vero e proprio successivamente all'operazione di verifica della propria identità.

Vi è, inoltre, la casistica in cui il recapito di una comunicazione dal mittente al destinatario avviene nel perimetro di una piattaforma proprietaria accessibile con autenticazione tramite certificato.

La garanzia di avvenuta consegna della comunicazione può assumere, allo stesso modo, diverse forme: il fondamento, come previsto dall'art. 44 eIDAS, è l'apposizione di una firma elettronica (almeno) avanzata o di un sigillo elettronico (al-

[13] La lista di fiducia è stata consultata il 20/04/2024.

meno) avanzato e di una marca temporale di tipo qualificato, i quali possono essere applicati a un documento elettronico (ad esempio in pdf o xml), il quale contiene i dati necessari a tracciare la trasmissione della comunicazione e i log delle operazioni effettuate dal destinatario.

È da evidenziare, però, come queste tipologie di recapito – rispetto alla PEC – possano risultare in alcuni ambiti meno trasversali: se, infatti, chiunque sia titolare di una casella PEC ad oggi può dialogare con il titolare di un'altra casella, indipendentemente dal Gestore che l'ha rilasciata a ciascuno degli attori, gli strumenti citati vedono il loro perimetro di azione tra il soggetto che li fornisce, il cliente che se ne avvale e il proprio bacino di utenti.

4. Il futuro del recapito elettronico e eIDAS 2.0: il punto focale dell'interoperabilità

Il Regolamento eIDAS 2.0, adottato dal Consiglio Europeo il 26 marzo 2024, non apporta novità sostanziali riguardo ai servizi di recapito elettronico; tuttavia, vi sono delle modifiche da esaminare.

La prima disposizione da porre il rilievo è il comma 8 dell'articolo 24a *Recognition of qualified trust services*: «A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States». Tale assunto rimedia all'assenza, nel primo eIDAS, di un esplicito riconoscimento transfrontaliero per questo specifico servizio.

L'articolo 43 resta invariato, mentre il 44 subisce gli emendamenti di seguito riportati. Viene aggiunto, al paragrafo 1, l'1a:

> 1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications and procedures referred to in paragraph 2.

Il paragrafo 2 viene interamente sostituito:

> 2. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2);
>
> 2a. Providers of qualified electronic registered delivery services may agree

> on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body. 2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be costeffective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

L'elemento che merita senz'altro una riflessione è l'importanza data all'aspetto dell'interoperabilità. L'aggiunta del paragrafo 2a, innanzitutto, è in accordo con quanto espresso nel considerando (52):

> Providers of qualified electronic registered delivery services should be encouraged by Member States to make their services interoperable with qualified electronic registered delivery services provided by other qualified trust service providers in order to easily transfer electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.

Il legislatore europeo ha dovuto – e dovrà, con gli atti implementativi – far fronte alla mancanza di protocolli comuni e alla peculiarità che contraddistingue ciascuno degli attuali mezzi di recapito sviluppati nei vari Stati dell'Unione. Se, infatti, per quanto riguarda altri servizi in esso regolamentati (quale, ad esempio, la sottoscrizione elettronica) l'eIDAS del 2014 ha raggiunto l'obiettivo di facilitare le transazioni transfrontaliere, lo stesso non può dirsi in relazione al tema dei recapiti elettronici. Resta la necessità non risolta di uniformare le modalità di trasferimento di dati elettronici tra due o più fornitori, in particolare se stabiliti in Stati differenti.

Un esempio concreto di questa problematica è riscontrabile nel caso d'uso dei recapiti elettronici qualificati nel contesto degli indici di domicilio digitale istituiti dalle Pubbliche amministrazioni. Questi, infatti, possono potenzialmente fungere da riferimento in un perimetro più ampio rispetto a quello della nazione entro la quale sono sviluppati. Se, infatti, l'apertura verso i QERDS da un lato si prospetta come opportunità, dall'altro potrebbe evidenziare i limiti dell'incompatibilità tra sistemi tecnologici differenti. Si pensi, in particolare, al contesto italiano: gli elenchi INI-PEC[14] e INAD[15], infatti, potrebbero dover registrare aziende, professionisti o privati cittadini

[14] L'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata è disponibile al link <https://www.inipec.gov.it/web/guest> (ultima consultazione: 20/04/2024).

[15] L'Indice Nazionale dei Domicili Digitali è disponibile al link <https://domiciliodigitale.gov.it/dgit/home/public/#!/home> (ultima consultazione: 20/04/2024).

che possiedono un servizio di recapito qualificato in un qualsiasi stato dell'Unione, che non risulterebbe, però, utilizzabile agli scopi di ricezione di comunicazioni per cui gli elenchi stessi sono stati concepiti[16].

In conclusione, operando un bilancio su quello che potrebbe essere l'impatto concreto di eIDAS 2.0 in Italia, si può affermare che il percorso dei recapiti elettronici qualificati sembri già tracciato, alla luce di quanto sin qui considerato: non si esclude un'apertura verso altri tipi di recapito più agili e meno vincolanti della PEC, ma il vero motore del cambiamento sarà senz'altro relativo al passaggio alla REM. È proprio questo standard, infatti, che dovrebbe portare all'obiettivo finale di interoperabilità su scala europea[17].

[16] Si veda, in proposito, il contributo G. Manca, *L'equivalenza tra PEC e SERCQ è un problema per il domicilio digitale: ecco perché*, «Agenda Digitale», 14 giugno 2023, disponibile al link <https://www.agendadigitale.eu/cittadinanza-digitale/lequivalenza-tra-pec-e-sercq-e-un-problema-per-il-domicilio-digitale-ecco-perche/> (ultima consultazione: 20/04/2024).

[17] Si veda, in proposito, il contributo G. Manca, *Il crepuscolo della PEC: arriva la REM, ecco cos'è e come funziona*, «Agenda Digitale», 03 giugno 2023, disponibile al link <https://www.agendadigitale.eu/documenti/il-crepuscolo-della-pec-arriva-la-rem-ecco-cose-e-come-funziona/> (ultima consultazione: 20/04/2024).

N. 4 - 2024 - pp. 235-240

La firma elettronica qualificata gratuita nel Portafoglio Europeo di Identità Digitale

Giovanni Manca

Abstract [IT]: Il regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale stabilisce regole per cui i Portafogli Europei di Identità Digitale "*offrono a tutte le persone fisiche la possibilità di firmare mediante firme elettroniche qualificate per impostazione predefinita e gratuitamente*". Il Legislatore comunitario, tenendo in conto lo stato del mercato privato delle firme elettroniche qualificate nel mercato interno, stabilisce anche una possibile deroga agli Stati membri che "*possono prevedere misure proporzionate per garantire che l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche sia limitato a scopi non professionali*".

L'applicazione di queste disposizioni richiede un'analisi di vari elementi operativi. I più rilevanti sono le modalità operative di apposizione della sottoscrizione qualificata e le regole per limitare l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche ai soli scopi non professionali.

In questo articolo si descrivono i possibili scenari operativi, con le soluzioni tecnologiche che possono essere utilizzate per una corretta applicazione delle disposizioni del citato regolamento europeo.

Abstract [EN]: The regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework set up rules for which the European Digital Identity Portfolio offers "*all natural persons the ability to sign using qualified electronic signatures by default and free of charge*". The Community Legislator, taking into account the state of the private market for qualified electronic signatures in the internal market, also establishes a possible exemption to Member States which "*may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes*".

The application of these provisions requires an analysis of various operational elements. The most relevant are the operational methods to add the qualified signature and the rules to limit the free use of qualified electronic signatures by natural persons to non-professional purposes only. The possible operational scenarios are described here with the technological solutions that can be used for correct application of the provisions of the aforementioned European regulation.

Parole chiave: Regolamento 2024/1183 (eIDAS 2.0), Portafoglio Europeo di Identità Digitale, firma qualificata gratuita, standard, verifica della firma qualificata

Sommario: 1.La normativa europea di riferimento – 2.Firmare con il Portafoglio Europeo – 3.Le scelte di carattere economico – 4.Le limitazioni d'uso delle firme qualificate – 5.La verifica delle sottoscrizioni nel nuovo scenario – 6. Conclusioni

1. La normativa europea di riferimento

La regola comunitaria che stabilisce che tutte le persone fisiche titolari di un Portafoglio Europeo di Identità Digitale hanno la possibilità di firmare mediante firme elettroniche qualificate per impostazione predefinita e gratuitamente è il regolamento del Parlamento europeo e del Consiglio che modifica il regolamento n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea (nel seguito eIDAS 2.0). L'approccio del Legislatore comunitario è indirizzato dalla volontà che il titolare del Portafoglio possa svolgere una serie di operazioni in modo sicuro e con la massima protezione de dati personali utilizzando la propria identità digitale. Una chiara spiegazione dello specifico obiettivo che si vuole raggiungere è presente nelle premesse all'eIDAS 2.0. È noto che i "considerando" nelle premesse non sono legge ma certamente non può essere ignorato il loro contenuto chiarificatore delle scenario di riferimento. Il punto citato è il (19) del quale viene, di seguito, riportato lo specifico contenuto di interesse dell'argomento qui descritto:

> (19) *"…I portafogli europei di identità digitale dovrebbero inoltre consentire agli utenti di creare e utilizzare firme e sigilli elettronici qualificati accettati in tutta l'Unione. Una volta effettuato l'onboarding in un portafoglio europeo di identità digitale, le persone fisiche dovrebbero poterlo utilizzare per firmare con firme elettroniche qualificate, per impostazione predefinita e gratuitamente, senza dover sottostare a ulteriori procedure amministrative. Ciò dovrebbe altresì consentire agli utenti di apporre firme o sigilli ad asserzioni o attributi autodichiarati."*

Il testo di questo "considerando" è chiaro. La persona fisica, titolare del Portafoglio Europeo, appena svolte le procedure finali di attivazione del Portafoglio deve essere in grado di firmare utilizzando la firma elettronica qualificata cioè la tipologia di firma che è ha effetti giuridici equivalenti ad una sottoscrizione autografa come già stabilito nell'articolo 25, paragrafo 2 del regolamento n. 910/2014 non modificato con il testo di eIDAS 2.0.

In molti Stati membri, compresa l'Italia, il mercato delle firme è sviluppato e quindi il Legislatore comunitario ha recepito le proposte di deroga alla disposizione seguente che stabilisce le regole normative attuative del citato "considerando", (articolo 6-bis, paragrafo 5, lettera g)) i Portafogli Europei di Identità Digitale:

"g) offrono a tutte le persone fisiche la possibilità di firmare mediante firme elettroniche qualificate per impostazione predefinita e gratuitamente."

La deroga stabilisce che "*gli Stati membri possono prevedere misure proporzionate per garantire che l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche sia limitato a scopi non professionali*".

L'analisi del testo non sembra indicare una possibile limitazione sul numero di firme disponibili per il titolare del Portafoglio, il limite è per l'utilizzo per le sole finalità non professionali.

In questa sede si intende trattare solo le questioni tecnologiche quindi, iniziamo ad analizzare le operazioni di sottoscrizione qualificata con il Portafoglio Europeo per poi individuare le possibili limitazioni d'uso della sottoscrizione.

2. Firmare con il Portafoglio Europeo

Una firma qualificata è definita come una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Come tutte le regole nella legislazione comunitaria anche queste sono tecnologicamente neutre ma possiamo affermare in modo convinto allo stato dell'arte della tecnologia un Portafoglio Europeo non può disporre di una varietà adeguata di dispositivi per la creazione di una firma elettronica qualificata. Uno smartphone o un tablet che utilizzano l'APP realizzativa del Portafoglio possono adeguatamente svolgere i compiti associati all'identità digitale, ma non soddisfano diffusamente (in termini di disponibilità di mercato di dispositivi certificati per la creazione di una firma elettronica qualificata).

La conseguenza è che, come già avviene oggi, il Portafoglio sarà utilizzato per l'identificazione e l'autenticazione del titolare sottoscrittore ad un dispositivo che oggi è un HSM (Hardware Security Module). Questo apparato verificata l'identità mediante le funzionalità del Portafoglio lo autorizza a procedere nelle operazioni di sottoscrizione gestite completamente dall'HSM.

Quest'ultimo è in grado di generare la coppia di chiavi asimmetriche per la sottoscrizione e di associarle al certificato qualificato che può anche contenere le limitazioni d'uso previste dalla norma comunitaria.

Il tema delle limitazioni d'uso viene affrontato nel paragrafo 4, nel successivo paragrafo analizziamo le scelte di carattere economico relative alla gratuità delle firme qualificate.

Possiamo, in ogni caso, ipotizzare che la costante evoluzione tecnologica non esclude che, in tempi ragionevoli, lo smartphone o il tablet possano essere dei dispositivi validi per la creazione di firme qualificate. Questo sarà possibile con la tecnologia del cosiddetto *secure element* o della eSIM, trasformazione della classica SIM telefonica.

3. Le scelte di carattere economico

La norma comunitaria stabilisce un uso gratuito della firma elettronica qualificata da parte del titolare del Portafoglio Europeo di Identità Digitale. Qualcuno deve sostenere l'onere economico di un utilizzo gratuito. Ipotizziamo gli scenari più probabili, partendo dai modelli di business già presenti.

La firma elettronica qualificata è un servizio. Questo servizio è offerto "monouso" o per un periodo collegato alla durata della validità del certificato qualificato.

Per l'utilizzo "a periodo" si può sottoscrivere un contratto senza limiti nel numero di creazioni di firma qualificata. Nel caso di sottoscrizione con procedura automatica l'elevato numero di firme prodotte cambia la tariffazione ma un uso non professionale non utilizza certamente questa modalità di sottoscrizione.

In attesa di interventi chiarificatori della Commissione, ma anche degli Stati membri, ipotizziamo che sono gratuiti l'attivazione del servizio di firma (il Portafoglio ne è dotato per "*impostazione predefinita*" quindi sembra dover essere dotato anche del certificato digitale) e il suo utilizzo per scopi non professionali.

L'attivazione di un Portafoglio porta anche all'attivazione del servizio di firma che quindi deve essere disponibile nell'ecosistema del Portafoglio stesso. Come lo Stato (o un privato, visto che il Portafoglio può essere emesso da un soggetto privato) attiva questa opzione? Con una gara d'appalto su almeno un paio di fornitori del servizio? Eroga il servizio direttamente tramite un soggetto, ente pubblico, qualificato per l'emissione di certificati per le firme elettroniche?

La deroga consentita dal regolamento eIDAS 2.0 è una possibilità e non un obbligo per lo Stato membro, questo crea una situazione disomogenea a livello del mercato interno.

In tali confini bisogna definire cosa è un uso professionale per evidenziare l'uso non professionale.

Il "considerando" (19) parla di firme di asserzioni e attributi autodichiarati ma certamente un cittadino che firma un documento verso le pubbliche amministrazioni firma gratuitamente, l'uso non professionale è evidente. La firma di un commercialista verso l'Agenzia delle Entrate risulta ad uso professionale e quindi non è gratuita per impostazione predefinita.

Le scelte devono essere sancite in norme, anche nazionali, ma all'atto pratico dove verifichiamo che la firma di Mario Rossi è abilitata ad uso esclusivo non professionale? Lo facciamo con il certificato qualificato come descritto nel paragrafo seguente.

4. Le limitazioni d'uso delle firme qualificate

Gli standard da utilizzare per i certificati qualificati per le firme elettroniche sono stabiliti negli standard ETSI. Lo standard di riferimento per i certificati qualifi-

cati per le firme elettroniche è ETSI EN 319 412-1 recante il documento "*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures*" da utilizzare, visto lo specifico scenario insieme a ETSI EN 319 412-2 recante in documento "*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons*". Trattandosi di certificati qualificati è necessario fare riferimento anche standard ETSI EN 319 412-5 recante il documento "*Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*".

In Italia sono in già in vigore norme per le limitazioni d'uso stabilite nella Determinazione AgID 147/2019, in particolare:

> "eventuali ulteriori limiti d'uso sono inseriti nell'attributo *explicitText* del campo *userNotice* dell'estensione *certificatePolicies*. Sul sito istituzionale dell'Agenzia sono pubblicati i testi e le codifiche delle limitazioni d'uso che è auspicabile siano garantite agli utenti".

I testi proposti da AgID (anche in lingua inglese) sono i seguenti:

- I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.
- Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.
- L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto). The certificate may be used only for relations with the (declare the subject).

Non è complesso inserire nel certificato un ulteriore attributo per limitare l'uso dei certificati a scopi non professionali, il candidato più logico per contenere questa modifica è ETSI EN 319 412-5.

Vale la pena di ricordare che moltissimi prestatori di servizi fiduciari qualificati operano nel mercato professionale o esclusivamente per la pubblica amministrazione. In questi casi i certificati qualificati emessi sono nativamente per scopi professionali e quindi non conformi alle regole stabilite per il Portafoglio Europeo.

Proseguiamo la nostra analisi evidenziando che lo scenario della firma non professionale necessita di nuove modalità di verifica delle firme elettroniche qualificate. Questo è il tema del prossimo paragrafo.

5. La verifica delle sottoscrizioni nel nuovo scenario

Nel mondo reale quando si verifica una firma elettronica qualificata non è prassi comune la verifica delle estensioni del certificato tra le quali abbiamo la sopra descritta "limitazione d'uso". Si verifica che il certificato contenente la chiave pubblica del sottoscrittore sia un certificato qualificato, che il documento sia integro e si evidenzia che ha firmato il titolare, in modo congruo con gli scopi di valenza giuridica legale ed efficacia probatoria che devono essere attribuiti al documento informatico sottoscritto.

Se siamo nello scenario di utilizzo del Portafoglio Europeo è indispensabile verificare che la firma apposta sia coerente con lo scenario di utilizzo. Quindi chi ha l'onere legale di verificare la sottoscrizione dovrà controllare la firma elettronica qualificata anche comunemente nota come firma digitale e confermata la sua validità tecnologica dovrà verificare anche che il sottoscrittore ne abbia fatto un uso non professionale perché questo è indicato nelle limitazioni d'uso del certificato. La cosa non è facile da realizzare quando le verifiche sono effettuate con strumenti automatici. Non bisogna dimenticare anche la necessità di adeguare la normativa vigente sul tema della mancata sottoscrizione se non sono soddisfatti i limiti d'uso relativi all'uso non professionale della sottoscrizione.

6. Conclusioni

La possibilità per le persone fisiche titolari di un Portafoglio Europeo di Identità Digitale di poter firmare gratuitamente mediante firme elettroniche qualificate è un obbligo stabilito nel nuovo regolamento europeo eIDAS 2.0. Gli Stati membri possono limitare questo uso gratuito a scopi non professionali. Questa possibilità consente al cittadino di firmare documenti verso la pubblica amministrazione ma anche verso soggetti privati come, ad esempio, una banca quando sottoscrive un mutuo o una polizza di assicurazione sanitaria. Quando si opera in un mercato dove la vendita di servizi di firma qualificata è elevata si pongono una serie di problemi che devono essere risolti anche con scelte di politica economica e normative adeguate. Il testo specifico nel regolamento eIDAS 2.0 non è chiarissimo e si presta anche ad interpretazioni capziose ma non contraddittorie rispetto al testo della norma.

Saranno necessarie chiarimenti da parte della Commissione europea e dei Governi nazionali, ai quali spettano anche l'eventuale attivazione delle possibilità offerte dal regolamento.

Al momento si può solo auspicare l'impatto positivo sui cittadini della possibilità di sottoscrivere gratuitamente documenti informatici con grande beneficio per la digitalizzazione nel settore pubblico e in quello privato.

N. 4 - 2024 - pp. 241-250

Autori di questo numero

Simone Baldini
Esperto in firma digitale e PKI per la sicurezza informatica.
In qualità di esperto PKI e firma digitale con leadership nel team In.Te.S.A. SpA, ricopre un ruolo chiave nello sviluppo di servizi fiduciari qualificati e eIDAS.
Il suo gruppo di lavoro si occupa della gestione prodotti e certificazioni aziendali (eIDAS QTSP, eID) in ambito Servizi Fiduciari. Guida i progetti chiave per la sicurezza informatica e l'innovazione tecnologica. Ha sviluppato specifica esperienza in diversi settori: infrastruttura PKI: progettazione, implementazione e gestione di sistemi PKI sicuri e affidabili; firma digitale e smart card: tecnologie di firma digitale avanzata e sistemi di gestione delle smart card; gestione carte e provider di identità (SPID): sistemi di autenticazione forte e SPID per l'accesso sicuro ai servizi online; posta elettronica certificata (PEC): gestione di sistemi di PEC conformi alle normative vigenti; crittografia e moduli di sicurezza hardware (HSM): crittografia dei dati e protezione dei sistemi informatici con HSM; normativa e organizzazione PKI: conoscenza approfondita degli aspetti legali e organizzativi della PKI. È certificato: OPST (ISECOM); PRINCE2 Foundation & Practitioner (APMG); CCNA, CCSP (Cisco);CCSA (Check Point).
email: *simone.baldini@intesa.it*

Ernesto Belisario
Avvocato cassazionista, è specializzato in Diritto Amministrativo e Scienza dell'Amministrazione e si occupa di diritto delle tecnologie. È Senior Partner dello Studio Legale E-Lex, assistendo imprese e pubbliche amministrazioni in questioni relative al diritto delle tecnologie (digitalizzazione e dematerializzazione, open government, open data, privacy, startup, intelligenza artificiale). È docente in numerosi corsi di formazione e specializzazione e autore di numerose pubblicazioni nelle materie di attività. È stato Consigliere del Ministro per la Semplificazione e la pubblica amministrazione, componente del Tavolo permanente per l'innovazione e l'agenda digitale della Presidenza del Consiglio dei Ministri e Componente della commissione degli utenti dell'informazione statistica costituita presso ISTAT. Ha fatto parte della Task force sull'intelligenza artificiale costituita dall'Agenzia per l'Italia Digitale che nel 2018 ha pubblicato il "Libro Bianco" su "Intelligenza artificiale al servizio del cittadino".
È curatore del progetto lapadigitale.it.
email: *ebelisario@e-lex.it*

Andrea Caccia
Ingegnere con una lunga e consolidata esperienza nello sviluppo e nell'applicazione di standard nell'ambito dell'identificazione elettronica, dei servizi fiduciari e della digitalizzazione in generale. Dal 2015 partecipa in rappresentanza di Small Business Standards (SBS), l'associazione europea per la difesa degli interessi delle PMI nella standardizzazione, ai lavori dei principali comitati tecnici responsabili dello sviluppo degli standard a supporto del regolamento eIDAS presso gli enti di normazione europei ETSI e CEN. In ambito ETSI, in particolare, ha contribuito attivamente allo sviluppo del framework di standard a supporto dei servizi fiduciari e delle firme elettroniche, inclusi gli standard sui formati di firma e sui servizi elettronici di recapito certificato.
A livello nazionale partecipa attivamente alle attività di numerosi organismi tecnici dell'ente di normazione UNI e dell'ente federato UNINFO, presiedendo in particolare il sottocomitato SC FIS, firme, identità e sigilli elettronici e relativi servizi, e il comitato sulla blockchain e i registri distribuiti. Dal 2014 è presidente del comitato tecnico europeo CEN/TC 434 sullo sviluppo degli standard sulla fatturazione elettronica. Negli stessi ambiti svolge attività di consulenza per enti pubblici e privati.
email: *andrea.caccia@studiocaccia.com*

Davide Colletto
È un imprenditore con oltre 20 anni di esperienza nel settore della gestione documentale e dei sistemi per la conservazione a norma dei documenti a livello internazionale. Si occupa di normativa eIDAS, che regola i servizi fiduciari elettronici nell'Unione Europea, e di Blockchain, Ha fondato ed è attualmente investitore e consulente di diverse startup nel mondo della digital transformation e blockchain. Attualmente Davide Coletto è il CTO di Namirial SPA, una società leader nel mercato dei servizi fiduciari elettronici, che offre soluzioni di firma digitale, identificazione elettronica, conservazione digitale, fatturazione elettronica e sicurezza informatica. In questa posizione, coordina le attività di ricerca e sviluppo, gestisce i progetti strategici e supervisiona la qualità dei servizi offerti.
email: *d.coletto@namirial.com*

Andrea De Maria
Ingegnere elettronico, da sempre appassionato di microprocessori, ha sviluppato SIM card e altre applicazioni su smart card in ambito Telco per la Incard, società poi confluita in STMicroelectronics. In Francia ha lavorato allo sviluppo di applicazioni di firma digitale e di autenticazione, soprattutto per il mondo Banking. È passato poi al settore Government in Siemens, dove, tra l'altro, ha sviluppato la specifica tecnica della Carta Nazionale dei Servizi. All'Istituto Poligrafico e Zecca dello Stato dal 2006, si occupa di nuovi prodotti e nuovi servizi, tra cui Carta d'Identità Elettronica e i relativi servizi (identità digitale, firma digitale) e del Wallet.
email: *a.demaria@ipzs.it*

Giulio Di Clemente
Si laurea in Matematica all'Università Federico II di Napoli il 18/02/2020; subito dopo fa ingresso nella Bit4id s.r.l., oggi società del Gruppo Namirial, in cui lavora tuttora, con la mansione di R&D Analyst nella business unit "Innovation & Improvement". Si occupa principalmente di attività di standardizzazione a livello europeo sui temi legati ai servizi fiduciari e delle tematiche di Crittografia rilevanti per il Gruppo; è proprio tramite la Crittografia che approda al mondo delle blockchain e dei registri distribuiti, allo studio dei quali è legato il presente articolo.
email: *g.diclemente@namirial.com*

Flavio Fanton
Si occupa di Posta Elettronica Certificata (PEC) dal 2004, anno di avvio della sperimentazione del servizio in Italia. Ha fondato il progetto open source che implementa il flusso PEC adottato da più gestori, ha fondato inoltre una startup dedicata alla realizzazione di sistemi PEC ad alta prestazione. Attualmente ricopre il ruolo di responsabile del servizio PEC presso Namirial S.p.A., dove si dedica alla transizione per la qualifica del servizio secondo gli standard ETSI REM.
email: *f.fanton@namirial.com*

Luigi Foglia
Avvocato del Foro di Lecce, è partner dello Studio Legale Lisi dal 2009 e collabora con la Digitalaw S.r.l. occupandosi principalmente di diritto dell'innovazione digitale, contratti di outsourcing informatico, formazione e conservazione digitale del documento informatico, firme elettroniche, altri servizi fiduciari, fatturazione elettronica, innovazione nella PA, privacy, contratti IT, licenze d'uso software e disaster recovery. Attualmente è Segretario Generale di Anorc (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti). Iscritto nell'Elenco di ANORC Professioni dei "Professionisti della digitalizzazione" - Livello EXPERT. Ricopre il ruolo di Responsabile della Conservazione esterno per diverse aziende. Relatore in numerosi convegni nazionali e autore di pubblicazioni su note testate di settore in materia di diritto delle nuove tecnologie. Nelle materie di sua competenza ha fornito servizi di docenza e consulenza in favore di enti pubblici, società partecipate, aziende private.
email: *luigifoglia@studiolegalelisi.it*

Enrico Giunta
Laureato in Scienze storiche, ha conseguito il Master di II livello in Formazione, Gestione e conservazione di archivi digitali in ambito pubblico e privato, è Responsabile della Funzione Archivistica di Conservazione di Namirial Spa e Product Specialist della Business Unit "Archiving & Communications Solutions" sempre presso Namirial. Expert in ambito di archivi digitali, long-term archiving, conservazione a norma, compliance agli standard e al quadro normativo

nazionale ed internazionale, si occupa degli aspetti di definizione e gestione del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità. Product Specialist nella definizione dei requisiti di prodotto di archiviazione elettronica, conservazione a norma, fatturazione elettronica, recapiti elettronici. Gestisce attività legate al product lifecycle e al go-to-market. Fino al 2023 Project Manager di Namirial Spa nell'ambito dei Digital Trust Services dell'azienda: eSigning, eArchiving, Long Term Archiving & Preservation, eInvoicing, Onboarding, eIdentification, Certified Communication. Socio ANORC (Associazione Nazionale Operatori e Responsabili della Custodia di contenuti digitali) e Achivista inserito negli elenchi nazionali dei Professionisti dei Beni Culturali.
email: *e.giunta@namirial.com*

Donato A. Limone
Già professore ordinario di informatica giuridica; docente di diritto dell'amministrazione digitale e scienza dell'amministrazione digitale; ha insegnato nelle università di Camerino, Luiss, Salento, Federico II Napoli, Sapienza, Unitelma Sapienza. Esperto di organizzazione e digitalizzazione delle pubbliche amministrazioni. Fondatore e direttore della "Rivista elettronica di diritto, economia, management".
email: *donato.limone@gmail.com*

Andrea Lisi
Avvocato, si occupa di diritto applicato all'informatica da circa 25 anni. Oltre allo Studio Legale Lisi, coordina le realtà di Digitalaw e D&L NET. È il Presidente di ANORC Professioni e il Direttore del progetto editoriale DIGEAT. Dal 2024 è iscritto nell'Elenco dei Manager dell'Innovazione gestito da Unioncamere. Dal 2023 è Componente nel Comitato di Esperti di comprovata esperienza e qualificazione in materia di innovazione tecnologica e transizione digitale della PA che affianca il Sottosegretario alla Presidenza del Consiglio con delega all'Innovazione tecnologica, Sen. Alessio Butti per guidare la trasformazione digitale del Paese. Il 23 settembre 2022 e il 18 settembre 2023 è stato componente del Tavolo "DPO" dello "State of Privacy" fondato dall'Autorità italiana Garante per la protezione dei dati personali. È componente della lista tenuta dal Comitato europeo per la Protezione dei Dati "Experts for the implementation of the EDPB's Support Pool of Experts" relativamente ai settori "Technical expertise in new technologies and information security" e "Legal expertise in new technologies".
Riveste il ruolo di Direttore scientifico di numerosi Master e percorsi specialistici universitari di settore, organizzati in collaborazione con Università ed Enti di Formazione nazionali. Approfondisce quotidianamente - sviluppando consulenza, assistenza e formazione in favore di PA e Imprese nazionali - gli aspetti giuridici della digitalizzazione, della contrattualistica informatica, dell'e-

commerce e dell'e-gov, della sicurezza informatica e della protezione dei dati.
email: *andrealisi@studiolegalelisi.it*

Giovanni Manca
Ingegnere elettronico esperto di digitalizzazione, sicurezza informatica e trasformazione digitale. A partire dal 1986 si è occupato di identità digitale, dematerializzazione (conservazione e gestione) dei documenti informatici, sottoscrizioni informatiche, Digital Transaction Management, sicurezza informatica anche applicata al regolamento 679/2016 sulla protezione dei dati personali (GDPR). Nel periodo 1986-1999 ha lavorato in SOGEI per la digitalizzazione del sistema del Catasto, i servizi di rete fino alla messa in linea del primo sito di natura fiscale su Internet. Dal maggio 2001 fino all'aprile 2010 ha svolto attività direttive presso il Centro Tecnico per la RUPA, l'AIPA e il CNIPA. Tali attività hanno riguardato l'accreditamento e controllo delle aziende che operavano come certificatori di firma digitale o come gestori di posta elettronica certificata, il supporto tecnico al legislatore sulle problematiche di trasformazione digitale e la consulenza alle Pubbliche Amministrazioni sull'utilizzo sicuro dei servizi di rete e sulla integrazione nei flussi documentali di strumenti abilitanti come la firma o la PEC. Dal maggio 2010 ha proseguito le attività professionali come consulente in numerose aziende ICT. Dal dicembre 2015 è in LAND Srl dove è Responsabile della formazione e prosegue l già citate attività di consulenza. È coautore di norme primarie, come il Codice dell'Amministrazione Digitale, e delle normative tecniche in materia di firma digitale, conservazione documentale e documenti di identità digitale come la Carta Nazionale dei Servizi (CNS) e la CIE (Carta di Identità Elettronica). È docente in attività di alta formazione anche presso atenei e soggetti privati. Ha pubblicato centinaia di articoli sui temi della trasformazione digitale ed è autore dei libri "Le firme elettroniche" e "Memorie del digitale". Già Presidente di ANORC (Associazione Nazionale per Operatori e Responsabili della Custodia di contenuti digitali) nel biennio 2016-2018 è stato rieletto per il biennio 2022-2024.
email: *gmanca@land.it*

Marco Mangiulli
È CIO & Head of Software Development di Aruba S.p.A, e membro del CdA di Aruba PEC S.p.A. Da 7 anni in Aruba è Responsabile dello Sviluppo Software, guidando la progettazione e la realizzazione dei sevizi di Web Hosting, Registrazione Domini, Cloud Computing, eSecurity e Trust Services. Laureato al Politecnico di Torino in Ingegneria Informatica, si occupa da oltre 20 anni di standard e tecnologie relative alla sicurezza dei dati e delle informazioni, ed in particolare di Ethical Hacking, Crittografia, Public Key Infrastructure, Firme Elettroniche, Blockchain e Distributed Ledger, Sistemi di identificazione biometrica, Identità Digitale, PEC & Sistemi di eDelivery, e di strategie, metodi e tecnologie per la conservazione a lungo termine dei documenti elettronici. Numerose le

sue competenze informatiche, tra cui metodologie, strumenti e tecnologie per la progettazione e la realizzazione di applicativi moderni basati su architetture a micro-servizi ed approccio cloud native. Da luglio 2023 ricopre anche il ruolo di Amministratore e Chief Technology Officer di ArubaKube, spin-off del Politecnico di Torino e polo di eccellenza per lo sviluppo del cloud native.
email: *marco.mangiulli@staff.aruba.it*

Igor Marcolongo
Manager specializzato nella trasformazione digitale dei processi di business mediante i servizi fiduciari, ha gestito con successo numerosi progetti in ambito firma elettronica, *onboarding* digitale, *eDelivery* e archiviazione digitale in contesti nazionali e internazionali.
Ha costituito e coordinato la *practice* di *business compliance* del Gruppo InfoCert, presidiando le evoluzioni delle normative nazionali ed europea sui servizi fiduciari e l'identità digitale e coordinando le analoghe attività delle controllate.
Membro del board e dell'Advocacy Commitee di CSC – *Cloud Signature Consortium*, del Consiglio Direttivo di AssoCertificatori e di ESD – *European Signature Dialog*, collabora con numerose associazioni e *think tank* a livello internazionale.
Conseguito l'Executive MBA presso l'Università degli Studi Tor Vergata di Roma, ricopre oggi il ruolo di Head of Business Evolution in InfoCert SpA, con responsabilità sulle attività di marketing di gruppo, comunicazione, analisi e formulazione strategica, analyst relations e relazioni istituzionali a livello globale.
email: *igor.marcolongo@infocert.it*

Marti Federica
Dottoressa di ricerca in *Memorie e Digital humanities*, con tesi e progetto di ricerca dal titolo "Disposizioni normative, modelli e strumenti per la conservazione di documenti e archivi digitali in Italia e in Europa: panorama complessivo, casi di studio, analisi comparata e prospettive", ha conseguito anche il Master di Master di II livello in Formazione, Gestione e conservazione di archivi digitali in ambito pubblico e privato. È attualmente *Regulatory compliance & audit specialist* presso Namirial S.p.A. e si occupa della conformità dei servizi erogati dall'azienda (identità elettronica SPID, certificati di firma e sigillo qualificati, marche temporali, conservazione a lungo termine, Posta Elettronica Certificata, soluzioni di *onboarding* da remoto), alle disposizioni nazionali ed europee vigenti, nonché delle analisi dei nuovi provvedimenti. Inoltre, insieme al proprio team e le funzioni aziendali di competenza, coordina le certificazioni di sistema ISO 9001, ISO 27001 con estensioni 27017 e 27018, ISO 37001, UNI PdR 125:2022 e dei servizi sopra elencati, nonché gli audit interni ad essi relativi.
email: *f.marti@namirial.com*

Massimiliano Nicotra
Avvocato, Senior Partner di Qubit Law Firm & Partners. Si occupa di diritto della tecnologia e protezione dei dati personali da oltre venti anni. È Data Protection Officer di società nazionali e multinazionali e professore a contratto in "Diritto e gestione della pubblica amministrazione digitale" presso l'Università Europea di Roma.
Coordinatore della sezione Privacy e Compliance del Centro di Ricerca Economica e Giuridica (CREG) nonché Vicepresidente del Comitato Strategico del Centro di Ricerca sull'Amministrazione Digitale (CRAD) presso l'Università degli Studi di Roma Tor Vergata, Dipartimento di Management e diritto e docente nel corso di alta specializzazione in Responsabile della protezione dei dati e sicurezza delle informazioni.
Attualmente ricopre la carica di componente del Comitato di Controllo del Polo Strategico Nazionale per conto della Presidenza del Consiglio dei Ministri.
Co-founder del chapter romano dei Legal Hackers.
È autore di numerosi contributi in materia di diritto della protezione dei dati personali, diritto dell'informatica e amministrazione digitale, fintech e diritto bancario.
email: *nicotra@studionicotra.com*

Adriano Santoni
Responsabile dello Sviluppo dei servizi di Certification Authority e Time-Stamping di Aruba S.p.A. Laureato in Ingegneria presso il Politecnico di Milano, si occupa di PKI da più di 20 anni, avendo guidato la realizzazione e l'accreditamento della prima CA pubblica italiana (SIA S.p.A., nel 2000), e successivamente quella di Actalis S.p.A. (2002). In seguito ha coordinato lo sviluppo di prodotti software per la firma digitale e progetti relativi alla Carta Nazionale dei Servizi. Dopo l'acquisizione di Actalis da parte di Aruba, nel 2009, ha svolto anche attività di pre-sales e di project management, con particolare focus sugli stessi temi, per poi riassumere nel 2016 la responsabilità dei servizi fiduciari (trust services). Dal 2011 si è dedicato particolarmente all'evoluzione dei servizi di CA "publicly trusted", occupandosi anche di aspetti di compliance e di product management. Rappresenta Actalis nell'ambito del CA/Browser Forum sin dal 2014 e nei relativi gruppi di lavoro che sviluppano gli standard tecnico-operativi della WebPKI. Svolge saltuariamente anche attività di consulenza e formazione, interna ed esterna.
È' l'autore della specifica pubblica RFC 5544. Ha conseguito la certificazione CISSP. Nel suo tempo libero si dedica al trekking, alla musica e alla lettura.
email: *adriano.santoni@staff.aruba.it*

Andrea Sassetti
Amministratore Delegato di Aruba PEC S.p.A. e Direttore Trust Services del Gruppo Aruba. Da oltre 23 anni si occupa di servizi fiduciari qualificati, di pro-

getti legati all'identità digitale e di processi di dematerializzazione. È Presidente di AssoCertificatori, socio sostenitore ANORC, ETSI, ESD e Cloud Signature Consortium, partecipando attivamente ai tavoli di lavoro su compliance normativa e interoperabilità delle soluzioni sia in ambito italiano che europeo.
email: *andrea.sassetti@staff.aruba.it*

Patrizia Sormani
Expert digital manager vanta una formazione poliedrica: Laurea in Economia e Commercio presso l'Università Bocconi di Milano e Laurea in Giurisprudenza presso l'Università Statale sempre di Milano.
Da oltre un decennio fornisce consulenza in genere nel settore dell'ICT e del diritto applicato all'informatica ed in particolare: nel settore dei servizi fiduciari (QTSP- quality trust service provider), della gestione documentale, della conservazione digitale e dei processi di digitalizzazione in genere, delle firme elettroniche, dei sistemi di autenticazione; nel settore di supporto ed assistenza sui temi del diritto applicato all'informatica declinati dal Codice dell'Amministrazione Digitale, Regolamento eIDAS coadiuvando nella predisposizione della documentazione inerente ai servizi digitali e fiduciari, anche a supporto del Responsabile della Gestione Documentale e del Responsabile della Conservazione; nel settore dei processi di dematerializzazione documentale massiva degli archivi cartacei supportati da "certificazione di processo"; nel settore dell'ideazione, sviluppo, implementazione e realizzazione di soluzioni e piattaforme digitali e nella digital transformation in genere, occupandosi di digital project management al fine di supportare le analisi di processi e work flow digitali per seguire step by step l'iter della loro realizzazione; nel settore dell'analisi e sviluppo di business a supporto della diffusione e commercializzazione di soluzioni a elevato contenuto tecnologico, applicazioni e servizi per la sicurezza dei dati, prodotti avanzati nell'ambito delle firme elettroniche, della gestione dell'identità digitale e dell'autenticazione multifattoriale, della gestione digitale delle transazioni di approvazione e firma documenti, della crittografia e protezione dati nonché nella conservazione digitale.
È impegnata in diverse attività di docenza Master in ambito di digitalizzazione dei processi operativi e formazione in collaborazione con alcune organizzazioni di alta formazione manageriale presenti in Italia nonché in formazione diretta presso società ed enti. Ha una pluriennale esperienza di docenza presso il dipartimento di diritto amministrativo dell'università del Molise di Campobasso e fa parte del comitato di indirizzo della laurea in Gestione e Conservazione dei Documenti digitali presso l'Università della Calabria.
email: *sormani@patriziasormaniconsulting.com*

Beatrice Tafini
Legal Counsel presso la società Intesi Group S.p.A., in precedenza, ha lavorato come Giurista d'impresa presso la società Intesa (an IBM company). Laurea

magistrale in Giurisprudenza con compiuta pratica forense presso studio che opera esclusivamente nel diritto amministrativo, con focus sulla contrattualistica pubblica, le società a partecipazione pubblica, l'urbanistica e i beni culturali. Nel suo percorso professionale ha maturato una solida esperienza in materia di diritto commerciale, contrattualistica d'impresa e del diritto societario. In parallelo si è dedicata alla compliance normativa dei servizi c.d. Fiduciari Qualificati e mezzi di identificazione elettronica erogati dalle società per cui ho operato acquisendo anche competenze specifiche in materia di Protezione dei dati personali.
email: *beatrice.tafini@intesigroup.com*

Sarah Ungaro
Avvocato - consulente senior, esperta in diritto dell'informatica e protezione dei dati. Collabora con lo Studio Legale Lisi in qualità di consulente senior in materia 20 di diritto dell'informatica, protezione dei dati personali, e-government, contratti IT, e-health, conservazione digitale e e-procurement. In relazione a tali materie, è docente per Università ed enti di formazione specialistica pubblici e privati, partecipa in qualità di relatrice a seminari e convegni ed è autrice di numerose pubblicazioni su testate specialistiche di settore. Vice Presidente dell'associazione ANORC Professioni, ne è componente della Commissione di valutazione ed è iscritta nell'Elenco della sezione "Professionisti della digitalizzazione" – Livello EXPERT e nell'Elenco della sezione "Professionisti della privacy" – Livello EXPERT, tenuti dalla stessa associazione. Ha svolto incarichi di docenza per conto di Università ed enti di formazione specialistica, tra cui: Università degli Studi di Bari – Dipartimento di Informatica, Università degli Studi di Roma Unitelma Sapienza, Scuola Umbra di Amministrazione Pubblica. Attualmente è tra i docenti del Corso di perfezionamento in Information security, Data protection, Digital forensics – I edizione – A.A. 2022/2023, organizzato da UNISOB. Ha partecipato in qualità di autrice alla redazione del Syllabus "Competenze digitali per la PA" il documento realizzato dal Dipartimento della funzione pubblica nell'ambito del progetto "Competenze digitali per la PA" – giunto alla sua seconda edizione (febbraio 2022). Autrice di numerose pubblicazioni su testate specialistiche di settore, tra cui: Sole24Ore (PA24, Professioni e Imprese24, Guida al pubblico impiego), ForumPA, Agendadigitale.eu, Corcom – Corriere Comunicazioni, Information Security, Il Documento Digitale, Diritto.net, Finanza e Diritto, e-Health, e-Cloud, Document Management System, Trust&Wealth Management Journal, ICT for Executive, Key4Biz, Filodiritto.
email: *sarahungaro@studiolegalelisi.it*

Andrea Valle
Studia ingegneria elettronica al Politecnico di Milano. Si specializza nell'ambito del documento elettronico, realizzando la prima soluzione di revisione collaborativa a distanza. Entra in Adobe nel 1998 come uno dei primi esperti del forma-

to PDF. Assume ruoli nel business development, contribuendo alla rivoluzione del documento elettronico non solo in ambito tecnologico, ma anche normativo e della standardizzazione. Si occupa di firma digitale e ne promuove l'adozione grazie all'uso nativo nel formato PDF. Nel 2006 contribuisce al riconoscimento di tale formato da parte del CNIPA, aprendo la strada alla pubblicazione dello standard PAdES da parte di ETSI (European Telecommunications Standards Institute).
Attualmente è responsabile dello sviluppo delle soluzioni di identità digitale e firma digitale per i prodotti Adobe, tra cui Acrobat e la piattaforma cloud Acrobat Sign. È anche direttore del programma Adobe Approved Trust List (AATL) che rappresenta l'unica lista globale di fornitori affidabili di certificati digitali per la firma elettronica documentale.
Rappresentante di Adobe presso ETSI, sviluppa gli standard globali per le firme elettroniche e l'identità digitale. Collabora allo sviluppo dello standard di firma ETSI EN 319 142 (PAdES) ed è esperto del Regolamento UE n. xxx/2024 (eIDAS) già dalla sua prima pubblicazione nel 2014. Nel 2016 fonda il Cloud Signature Consortium, associazione no-profit che sviluppa lo standard di riferimento per la firma digitale nel Cloud, e ne diviene il primo Presidente. Attualmente è membro del consiglio di amministrazione dell'associazione, che riunisce più di 70 membri da tutto il mondo.
email: *avalle@adobe.com*

CLIOeDU®

Soluzioni digitali d'*eccellenza* per progetti di prestigio

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOeDU®

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente.

INQUADRA IL QR-CODE PER IL DOWNLOAD DEGLI ALTRI NUMERI

www.clioedu.it/rivistaelettronica