Introduzione

Francesco Delfini e Giusella Finocchiaro [*]

SOMMARIO: 1. Il Regolamento e in particolare l'attuale quadro normativo italiano in tema di firme elettroniche. – 2. L'identificazione. – 3. Le firme elettroniche. – 4. I servizi fiduciari. – 5. I tratti fondamentali del Regolamento.

1. Il Regolamento e in particolare l'attuale quadro normativo italiano in tema di firme elettroniche

Il Regolamento in commento ("*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*") costituisce, dalla data di sua data di applicazione –: il 1° luglio 2016, salvo limitate eccezioni, come indicato nell'art. 52 – la disciplina generale, uniforme a livello europeo, dell'impiego, a fini negoziali, di strumenti informatici e telematici [1].

Il considerando 2 esplicita la finalità principale del Regolamento, di fornire «*una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico, nell'Unione europea*», nella consapevolezza che la precedente «*direttiva 1999/93/CE del Parlamento europeo e del Consiglio trattava le firme elettroniche senza fornire un quadro transfrontaliero e transettoriale completo per transazioni elettroniche sicure, affidabili e di facile impiego*» (considerando 3).

La precedente regolamentazione delle firme elettroniche, per lo strumento prescelto, quello della Direttiva (1999/93/CE), aveva richiesto norme di attuazione interna, avvenuta inizialmente con il d.lgs. 23 gennaio 2002, n. 10 e poi con le norme contenute nel Codice dell'Amministrazione digitale (d.lgs. 7 marzo 2005, n. 82, più volte novellato).

Ora il legislatore europeo, per rafforzare ed estendere l'*acquis* di tale direttiva – che viene contestualmente abrogata – ha preferito lo strumento del regolamento: e, come è noto, «*Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri*» (art. 288 co. 2, TFUE).

---

[*] Le opinioni espresse nell'introduzione sono integralmente condivise dagli autori. Tuttavia si precisa che il paragrafo 1 è stato scritto dal Prof. Francesco Delfini e i paragrafi 2-3-4-5 dalla Prof.ssa Giusella Finocchiaro.

[1] I lavori di stesura del presente volume sono cominciati prima della data di entrata in vigore del Regolamento. Per questa ragione, talora si fa riferimento a tale data al futuro. Tuttavia, il volume è aggiornato al d.lgs. 26 agosto 2016. n. 179.

La disciplina di settore recata dal Regolamento in parte innova ed in parte aggiorna e dettaglia quella contenuta nel CAD che era stato in passato modificato in attuazione della Direttiva 1999/93/CE, ora abrogata.

La legge 7 agosto 2015, n. 124, contenente «*Deleghe al Governo in materia di riorganizzazione delle amministrazioni pubbliche*», prevede una novellazione delegata per il CAD. L'art. 1 della legge 7 agosto 2015, n. 124 – intitolato "Carta della cittadinanza digitale", a conferma del più ampio oggetto della legge delega, non limitata al solo diritto privato dell'informatica – prevede che: «*1. Al fine di garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici, il Governo è delegato ad adottare, entro dodici mesi dalla data di entrata in vigore della presente legge, con invarianza delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, uno o più decreti legislativi volti a modificare e integrare, anche disponendone la delegificazione, il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, di seguito denominato "CAD", nel rispetto dei seguenti principi e criteri direttivi*: (...)». Tra tali principi e criteri direttivi spiccano, per quanto qui di interesse, quelli indicati alle lettere o-p) come segue: «*o) adeguare il testo delle disposizioni vigenti alle disposizioni adottate a livello europeo, al fine di garantirne la coerenza, e coordinare formalmente e sostanzialmente il testo delle disposizioni vigenti, anche contenute in provvedimenti diversi dal CAD, apportando le modifiche necessarie per garantire la coerenza giuridica, logica e sistematica della normativa e per adeguare, aggiornare e semplificare il linguaggio normativo e coordinare le discipline speciali con i principi del CAD al fine di garantirne la piena esplicazione; p) adeguare l'ordinamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche*».

Con il d.l. 26 agosto 2016 n. 179 il legislatore interno ha dunque esercitato tale delega per novellare ancora una volta il CAD – pur non disponendone la delegificazione – (anche) a seguito del Regolamento.

In particolare, l'art. 24 del CAD, che disciplina la firma digitale, è stato raccordato con il Regolamento, prevendo un co. 4-*ter* secondo cui «*Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni: a) il certificatore possiede i requisiti previsti dal regolamento eIDAS ed è qualificato in uno Stato membro; b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui al medesimo regolamento; c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali*».

In tema di documentazione informatica, poi, nel nuovo CAD si segnala la previsione della normale digitalizzazione di tutti gli atti pubblici – ferma la disciplina dell'atto pubblico notarile informatico, di più risalente previsione (d.l. 2 luglio 2010, n. 110), con estensione della equiparazione, già ivi prevista, della acquisizione in via informatica della firma autografa della parti apposta in presenza del pubblico ufficiale alla firma elettronica qualificata o digitale. L'art. 18 del d.l. 26 agosto 2016, n. 179 ha infatti inse-

rito il seguente co. 2-*ter* nell'art. 21 del CAD: «*2-ter. Fatto salvo quanto previsto dal decreto legislativo 2 luglio 2010, n. 110, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti».*

Ancora, la novellazione del CAD si segnala per l'introduzione all'art. 23, norma che tratta delle copie analogiche di documenti informatici, di un nuovo co. 2-*bis* che prevede l'equipollenza alla sottoscrizione autografa del pubblico ufficiale, di contrassegni a stampa[2] che rinviino all'originale documento informatico: *«2-bis. Sulle copie analogiche di documenti informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con le regole tecniche di cui all'articolo 71, tramite il quale è possibile accedere al documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa del pubblico ufficiale e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità».*

Per tornare alle materie disciplinate dal Regolamento, sulla base dell'art. 2 si può osservare, in primo luogo, che esso costituisce la nuova disciplina di principio delle firme elettroniche e dell'imputazione giuridica del documento informatico, sia nei rapporti tra il cittadino e la P.A., sia nei rapporti tra privati salvo che (art. 2.2) si tratti di servizi fiduciari (tra cui rientrano le firme elettroniche) «utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti».

In secondo luogo, è condivisibile la scelta (peraltro una scelta diversa non sarebbe stata praticabile alla luce dei principi del diritto europeo), del legislatore europeo, di «non pregiudica[re] il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma» (art. 2.3). Tale scelta si inserisce sulla già adottata opzione del legislatore interno che ha preferito non introdurre una nuova disciplina generale sulla conclusione del contratto per via telematica, richiamando invece le norme generali, specie codicistiche, sul tema (art. 1326 ss. c.c.), neutre quanto al modo di estrinsecazione della dichiarazione contrattuale. In questo senso deve infatti leggersi l'art. 13 del d.lgs. 9 aprile 2003, n. 70, di attuazione della Direttiva 2000/31/CE sul commercio elettronico, il cui primo comma ha tolto ogni dubbio in ordine alla soggezione dei contratti telematici alle norme di cui agli artt. 1326 ss. c.c.: «1. Le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica[3]».

---

[2] Si può pensare ad un codice QR (QR Code: *Quick Response Code*), già di comune impiego per richiamare pagine web o oggetti informatici partendo dalla scansione fotografica di una parte del documento a stampa.

[3] L'art. 13 del d.lgs. 9 aprile 2003, n. 70, rubricato "Inoltro dell'ordine", ha dato attuazione all'art. 11 della Direttiva 2000/31/CE, che completava la Sezione 3 dedicata ai contratti telematici, la cui defini-

2. L'identificazione

Il Regolamento distingue fra "identificazione elettronica" e "autenticazione elettronica".

L'identificazione elettronica (*electronic identification*) viene definita come il procedimento di utilizzo dei dati personali identificativi in forma elettronica al fine di rappresentare in modo univoco una persona fisica o giuridica, o la persona fisica che rappresenta una persona giuridica; mentre l'autenticazione (*authentication*) è definita come il processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, o l'origine e l'integrità dei dati in forma elettronica.

Nell'ordinamento giuridico italiano, invece, e segnatamente nel d.lgs. 7 marzo 2005, n. 82, Codice dell'Amministrazione digitale (di seguito più brevemente "CAD"), l'identificazione informatica era definita come la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, consentendone l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso (art. 1, co. 1, lett. u-*ter*). L'autenticazione, invece, non era[4] riferita al soggetto che accede al sistema informatico, ma al documento informatico. Essa era definita come la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione (art. 1, co. 1, lett. b). Entrambe le definizioni sono state eliminate dal CAD con il d.lgs. 26 agosto 2016, n. 179.

Una definizione più generale di autenticazione informatica è contenuta all'interno del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, art. 4, co. 3, lett. c), ove l'autenticazione è definita come l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Con riguardo agli strumenti di identificazione *on line*, il Regolamento dispone che gli Stati membri hanno facoltà di notificare alla Commissione sistemi di identificazione che, una volta accettati dalla Commissione e pubblicati, devono essere riconosciuti da tutti gli Stati membri. L'Italia, per esempio, potrà notificare la carta di identità elettronica (CIE) e l'identificazione *on line* con essa effettuata sarà riconosciuta negli altri Stati membri.

È bene precisare che ogni Stato può continuare ad utilizzare gli strumenti di identificazione *on line* già in uso e che in nessun modo il Regolamento impone l'adozione di uno strumento di identificazione *on line* comune europeo.

A seguito delle notifiche ricevute da parte degli Stati membri, la Commissione pubblica nella *Gazzetta Ufficiale* dell'Unione europea l'elenco dei sistemi di identificazione elettronica che sono stati notificati.

---

tiva formulazione aveva saggiamente abbandonato il proposito di uniformare in ambito europeo le regole sulla conclusione del contratto, limitando il contenuto dell'articolo alle modalità di inoltro dell'ordine.

[4] Giova ricordare che una precedente versione del CAD definiva l'autenticazione informatica come la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

Il Regolamento stabilisce le condizioni per la notificazione.

In particolare, un sistema di identificazione elettronica è ammissibile per la notifica, se tutte le condizioni di cui all'art. 7 sono soddisfatte. Dunque occorre che i sistemi di identificazione elettronica siano stati rilasciati dallo Stato membro notificante o riconosciuti dallo Stato e che i sistemi di identificazione elettronica siano utilizzati per l'accesso ad almeno un servizio fornito da un organismo pubblico dello Stato membro che effettua la notificazione.

Il Regolamento eIDAS prevede la responsabilità dello Stato membro notificante, della parte che rilascia i sistemi di identificazione elettronica e della parte che gestisce la procedura di autenticazione.

Se lo schema di identificazione notificato dallo Stato membro è pubblicato, ogni cittadino può usare il proprio sistema di identificazione elettronica negli altri Stati membri, attuando così il principio del riconoscimento reciproco dell'identificazione in materia di servizi *on line*.

Gli Stati membri possono ovviamente introdurre nuovi strumenti per l'identificazione elettronica per l'accesso ai servizi *on line*, ma sono tenuti a riconoscere gli strumenti che altri Stati hanno notificato alla Commissione europea.

Lo Stato notificante deve trasmettere alla Commissione una serie di informazioni relative al sistema di identificazione elettronica, compresa l'autorità responsabile per lo schema, all'emittente i sistemi di identificazione elettronica e al livello di garanzia prestato.

Il livello di garanzia dei sistemi di identificazione elettronica (basso, significativo o elevato) è determinato in base ai parametri di cui all'art. 8 del Regolamento eIDAS. I livelli di garanzia caratterizzano il grado di affidabilità che i sistemi di identificazione elettronica forniscono sull'identità dichiarata.

Il livello di sicurezza dipende dal processo di identificazione e di verifica, dall'attività svolta, dai controlli implementati anche sotto il profilo tecnologico.

L'obbligo di riconoscere *on line* un soggetto identificato in un altro Stato sussiste soltanto se il livello di sicurezza è almeno pari o superiore a quello richiesto dall'ente pubblico per accedere a tale servizio *on line* e se è almeno "significativo" o "elevato".

Se i sistemi di identificazione elettronica che vengono rilasciati nell'ambito di un regime di identificazione elettronica inclusi nell'elenco pubblicato dalla Commissione corrispondono al livello di garanzia "basso", gli enti pubblici hanno la facoltà di riconoscerli o meno ai fini dell'autenticazione transfrontaliera.

A ben vedere, non tutti i processi richiedono la modalità di identificazione più sicura che prevede, per esempio, la presenza fisica o la copia del documento di identità. Infatti, è diverso il livello di sicurezza dell'identificazione richiesto in banca o nell'*e-commerce*.

Il riconoscimento del sistema di identificazione *on line* che è stato accettato dalla Commissione è obbligatorio se l'interessato vuole identificarsi presso un soggetto pubblico (es.: partecipazione ad una gara d'appalto), mentre per i soggetti privati si tratta di una facoltà. Tuttavia si può facilmente prevedere che il settore privato avrà ogni interesse ad estendere il proprio mercato, avvalendosi di sistemi di identificazione *on line*.

Oltre alla necessità di garantire il riconoscimento reciproco dei sistemi di identificazione elettronica tra gli Stati membri, il Regolamento mira anche a garantire l'interoperabilità tecnica dei sistemi a livello dell'Unione.

Pertanto si afferma che i sistemi nazionali di identificazione elettronica notificati in conformità del Regolamento sono interoperabili e che deve essere istituito un quadro europeo di interoperabilità. Il Regolamento eIDAS prevede inoltre che la Commissione possa in seguito adottare atti di esecuzione del quadro di interoperabilità.

L'approccio scelto nel Regolamento è tecnologicamente neutro (fatto salvo quanto si dirà in commento all'art. 25): il quadro di interoperabilità non deve discriminare tra tutte le soluzioni tecniche nazionali specifiche per l'identificazione elettronica all'interno dello Stato membro e deve fare riferimento ai minimi requisiti tecnici di interoperabilità e ai minimi requisiti tecnici relativi ai livelli di sicurezza già citati.

Inoltre, al fine di agevolare la cooperazione tra gli Stati membri, è previsto che almeno sei mesi prima della notificazione del regime di identificazione elettronica alla Commissione, lo Stato membro notificante fornisca agli altri Stati membri una descrizione del sistema.

3. Le firme elettroniche

La parte del Regolamento dedicata alle firme elettroniche non comporta significative modifiche rispetto al quadro normativo previgente. A differenza di quanto accade per l'identificazione *on line*, in questo caso il legislatore europeo interviene in un ambito già consolidato [5].

È confermato il principio del non disconoscimento del documento informatico e delle firme elettroniche, secondo cui non può essere negata dignità e rilevanza giuridica ad una firma elettronica, solo in ragione della sua forma appunto elettronica. Secondo, infatti, l'art. 25, co. 1: «*alla firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova (...) per il solo motivo della sua forma elettronica*». È ribadito altresì, nel considerando 63 e nell'art. 44, che ad un documento elettronico non devono essere negati gli effetti giuridici per il solo motivo della sua forma elettronica. Il principio della irrilevanza della materia è finalizzato ad «*assicurare che una transazione elettronica non possa essere respinta per il solo motivo che il documento è in forma elettronica*».

Fra le innovazioni, si segnala che la firma elettronica è definita dall'art. 3 del Regolamento quale insieme di dati elettronici utilizzati "per firmare", diversamente da quanto previsto dalla direttiva del 1999 e dalla previgente versione del CAD, secondo cui la firma elettronica era costituita dall'insieme di dati elettronici utilizzati come metodo di identificazione informatica. Nella nuova versione del CAD, a seguito del d.lgs. 26 agosto 2016, n. 179, la definizione di firma elettronica è stata soppressa.

Non presentano connotati innovativi rispetto al dato normativo italiano, invece, le definizioni di firma elettronica avanzata e di firma elettronica qualificata, benché il citato d.lgs. n. 179/2016 abbia soppresso le definizioni.

In relazione alla definizione di firma elettronica avanzata è confermato il principio di neutralità tecnologica: la norma elenca una serie di condizioni, senza tuttavia impor-

[5] In materia si rinvia a G. FINOCCHIARO-F. DELFINI, *Diritto dell'informatica*, Utet, Torino, 2014.

re le modalità attraverso cui garantire il soddisfacimento di dette condizioni. Sempre con riguardo alla firma elettronica avanzata risulta, inoltre, confermata la necessità di garantire quattro requisiti e segnatamente che la firma sia connessa unicamente al firmatario, che sia idonea a identificare il firmatario, che sia creata con dati che il firmatario può con un elevato livello di sicurezza utilizzare sotto il proprio esclusivo controllo e che sia collegata ai dati sottoscritti in modo da rilevare ogni successiva modifica dei medesimi dati.

Sotto il profilo dell'efficacia probatoria, l'art. 25, co. 2, prevede un'automatica equiparazione, per gli effetti giuridici, della firma elettronica qualificata alla firma autografa.

È altresì confermato il principio del reciproco riconoscimento della firma elettronica qualificata, secondo cui una firma elettronica qualificata basata su un certificato qualificato rilasciato da uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Viene, infine, introdotto il sigillo elettronico che è un insieme di dati in forma elettronica acclusi, o connessi tramite associazione logica, ad altri dati in forma elettronica, per garantirne la provenienza e l'integrità. Si tratta di uno strumento per garantire l'integrità del documento, pur senza firma. Solo ad una prima lettura esso può essere considerato come la firma della persona giuridica: occorrerà valutare, infatti, alla luce dei singoli ordinamenti nazionali se si tratti di firma o meno. Anche in relazione al sigillo è affermato il principio secondo il quale ad un sigillo non possono essere negati effetti giuridici e probatori per il solo motivo della sua forma elettronica (art. 34, co. 1). Se qualificato, il sigillo gode della presunzione di integrità dei dati e di correttezza dell'origine dei dati a cui il sigillo è associato. I requisiti che devono soddisfare i certificati qualificati di sigillo elettronico sono oggetto di specifica elencazione nell'allegato III del regolamento.

Un quadro normativo, senza dubbio innovativo, che presenta diversi aspetti di rilievo ma che sotto il profilo generale del tema delle firme elettroniche non comporta modifiche sostanziali rispetto al panorama italiano.

4. I servizi fiduciari

L'ultima parte del regolamento è quella relativa ai cosiddetti "servizi fiduciari", o "*trust services*".

La definizione di servizio fiduciario è molto ampia e comprende molti dei servizi informatici offerti dal mercato. Si tratta, secondo il regolamento, di un servizio elettronico, fornito di norma a pagamento, consistente ne: «*(a) la creazione, la verifica e la convalida delle firme elettroniche, dei sigilli elettronici o validazioni temporali elettroniche, dei servizi elettronici di recapito certificato e dei certificati relativi a tali servizi; (b) la creazione, la verifica e la convalida dei certificati per l'autenticazione dei siti web, o (c) la conservazione delle firme elettroniche, sigilli o certificati relativi a tali servizi*».

Anche nel caso dei servizi fiduciari il legislatore opera una distinzione fra servizi qualificati e non qualificati. I servizi fiduciari qualificati sono esclusivamente quelli che soddisfano i requisiti indicati all'interno del regolamento stesso e che quindi si attestano ad un livello di sicurezza predeterminato: è richiesto un accertamento dei requi-

siti da parte dell'ente preposto e l'iscrizione in un apposito elenco, analogamente a quanto oggi accade per i certificatori qualificati.

Dopo aver ottenuto lo *status* di fornitore qualificato e l'iscrizione agli elenchi di fiducia, i fornitori di servizi qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.

I fornitori qualificati e non qualificati di servizi fiduciari devono predisporre appropriate misure tecniche e organizzative per gestire i rischi per la sicurezza dei servizi fiduciari che forniscono.

In particolare, il livello di sicurezza di tali misure deve essere commisurato al livello di rischio dell'attività.

È enfatizzato l'obbligo di comunicazione di eventuali incidenti occorsi, il cosiddetto "*data breach notification*", già presente nelle normative italiana ed europea. I soggetti destinatari dell'informazione possono essere l'interessato, l'Autorità per la protezione dei dati personali e l'ente competente in materia di sicurezza.

Se la violazione della sicurezza o la perdita dell'integrità del documento riguardano due o più Stati membri, è previsto il coinvolgimento dell'ENISA (*European Union Agency for Network and Information Security*).

Viene, come si è accennato, introdotto il sigillo elettronico che è strumento per garantire l'integrità del documento.

Anche con riferimento al sigillo elettronico, così come per le firme e per la validazione temporale elettronica e i documenti elettronici, viene sancito il principio di non discriminazione: al sigillo non può essere negato valore giuridico e il sigillo non può essere dichiarato inammissibile in giudizio unicamente perché in forma elettronica.

Come per le firme elettroniche si distinguono tre livelli di sigilli: semplici, avanzati e qualificati, in ragione dei requisiti di sicurezza.

Il Regolamento eIDAS introduce anche la cosiddetta "validazione temporale elettronica". Si tratta di un insieme di dati in forma elettronica che associano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento. La validazione temporale non attesta che il documento informatico è stato creato in quel preciso momento, ma semplicemente che esisteva in quella data e a quell'ora.

La marca temporale può essere sia "semplice" che "qualificata". La validazione temporale, si segnala, è un servizio già operante all'interno del nostro ordinamento.

Infine, il Regolamento prevede il cosiddetto servizio elettronico di recapito certificato che fornisce la prova di invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danneggiamento o eventuali modifiche non autorizzate.

Così come per gli altri servizi fiduciari, il servizio elettronico di recapito certificato prevede la forma qualificata, la quale crea la 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.

Nel nostro ordinamento la posta elettronica certificata (PEC) rappresenta il servizio elettronico di recapito certificato più diffuso.

Sono previsti, infine, i certificati di autenticazione del sito *web* che sono attestati che consentono di autenticare un sito *web* e di collegare il sito *web* alla persona fisica o giuridica cui è stato rilasciato il certificato, anch'essi nella forma semplice o qualificata. Lo scopo è quello di collegare il sito *web* ad una persona fisica o giuridica, garantendo, a livelli diversi la sua affidabilità.

5. I tratti fondamentali del Regolamento

Il Regolamento eIDAS si colloca nell'ambito della normativa europea volta a rafforzare la fiducia del mercato per potenziare il commercio elettronico che ha dato luogo, fra gli altri alla previgente direttiva sulle firme elettroniche. Rispetto alla normativa precedente, tuttavia, si distingue per lo strumento giuridico prescelto, quello del regolamento, che è idoneo a realizzare l'uniformazione e non solo l'armonizzazione del diritto europeo, nonché per l'ampia delega alla Commissione relativa alla normazione secondaria che darà corpo al Regolamento.

L'impatto del Regolamento sul quadro normativo italiano è ridotto, rispetto a quello che potrà avere su altri ordinamenti giuridici europei, perché essendo la legislazione italiana già ampiamente sviluppata in materia, la Commissione europea ha a questa ampiamente attinto.

L'obbligo del riconoscimento reciproco degli strumenti identificazione *on line*, o se si preferisce, la piena interoperabilità giuridica e tecnologica di questi, costituisce una importante innovazione. Non deve sfuggire, tuttavia, che tale obbligo è limitato al settore pubblico e che per i privati costituisce una facoltà.

Resta aperto il problema del riconoscimento dell'identità *on line* fuori dal mercato europeo, solo che si pensi a *provider* di prima grandezza nel commercio elettronico, quali la statunitense Google o la società cinese Ali Baba.

Capo I
Disposizioni generali

Articolo 1
Oggetto

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, il presente regolamento:

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

b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; e

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 e i servizi relativi ai certificati di autenticazione di siti web.

Articolo 2
Ambito di applicazione

1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, nonché ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

3. Il presente regolamento non pregiudica il diritto nazionale o unionale legato alla conclusione e alla validità di contratti o di altri vincoli giuridici o procedurali relativi alla forma.

Commento di

Andrea Dalmartello e Andrea Salvemini *

SOMMARIO: 1. Premessa: genesi e finalità del Regolamento eIDAS. – 2. Oggetto della nuova disciplina. a) L'identificazione elettronica. – 3. b) I servizi fiduciari. – 4. c) Firme elettroniche. – 5. d) Sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati di autenticazione di siti *web*. – 6. Ambito di applicazione e attuazione del Regolamento eIDAS. Rilievi conclusivi.

1. Premessa: genesi e finalità del Regolamento eIDAS

All'esito di un elaborato *iter* legislativo [1] è stato pubblicato sulla *Gazzetta Ufficiale dell'Unione europea* 28 agosto 2014, n. L 257 il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, recante la disciplina "*in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE*" [2].

Il Regolamento, conosciuto anche con l'acronimo eIDAS (*electronic IDentification Authentication and Signature*), è entrato in vigore il 17 settembre 2014 e sarà direttamente applicabile in tutti gli Stati Membri a decorrere dal 1° luglio 2016, fatte salve le eccezioni espressamente indicate, senza necessità di ulteriori atti di recepimento.

È senza dubbio significativa la scelta del legislatore UE di emanare un regolamento,

---

* Il presente contributo è frutto di riflessioni comuni degli autori. Tuttavia, i paragrafi 1, 5, 6 sono da attribuire ad Andrea Dalmartello e i paragrafi 2, 3, 4 sono da attribuire a Andrea Salvemini.

[1] Nelle conclusioni del 4 febbraio 2011 e del 23 ottobre 2011, il Consiglio europeo ha invitato la Commissione Europea a compiere entro il 2015 significativi progressi in settori chiave dell'economia digitale, nonché a promuovere un mercato unico digitale pienamente integrato che fosse in grado di facilitare l'utilizzo transfrontaliero dei servizi *on-line*, con particolare attenzione a garantire la sicurezza nelle procedure di identificazione elettronica e di autenticazione. Successivamente, nel comunicato stampa intitolato «*Digital "to-do" list: new digital priorities for 2013-2014*», la Commissione europea ha ribadito quanto segue: «*The digital economy is growing at seven times the rate of the rest of the economy, but this potential is currently held back by a patchy pan-European policy framework. Today's priorities follow a comprehensive policy review and place new emphasis on the most transformative elements of the original 2010 Digital Agenda for Europe. (...) Full implementation of this updated Digital Agenda would increase European GDP by 5%, or 1500€ per person, over the next eight years, by increasing investment in ICT, improving eSkills levels in the labour force, enabling public sector innovation, and reforming the framework conditions for the internet economy*». Così, nel mese di giugno 2012 la Commissione europea ha pubblicato una proposta relativa a una nuova normativa in materia di «*electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*»; e dopo lunga discussione in seno al Parlamento europeo e al Consiglio europeo, il Regolamento è stato adottato nel mese di luglio 2014.

[2] Per un primo commento al Regolamento, cfr. G. FINOCCHIARO, *Una prima lettura del reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, in *Nuove leggi civili comm.*, 2015, n. 3, p. 419 ss.

ai sensi dell'art. 114 TFUE, quale strumento normativo più idoneo ad assicurare maggiore efficacia e uniformità nell'applicazione della nuova disciplina su tutto il territorio dell'Unione. Si tratta di una evidente svolta rispetto al precedente approccio del legislatore comunitario, teso al ravvicinamento delle legislazioni nazionali mediante lo strumento dell'armonizzazione tramite la direttiva e strumenti di *soft law* [3].

È stato osservato che la ragione della scelta di utilizzare lo strumento regolamentare risiederebbe non solo nella peculiarità della materia oggetto della nuova normativa, ma anche, e soprattutto, nella mancanza durante la prima fase di sviluppo della c.d. "*e-europe*" di una base legale adeguata per il conseguimento da parte delle istituzioni europee dell'obiettivo di emanare una regolamentazione più efficace e puntuale [4]. Il Regolamento, adottato in attuazione dell'Agenda Digitale europea 2020 [5], costituisce il frutto della presa d'atto in seno alle istituzioni europee dell'eccessiva frammentazione del mercato interno dei servizi di identificazione digitale sicura, derivante dall'applicazione di norme diverse in ragione dello Stato membro in cui tali servizi erano erogati [6]. In particolare, è stato riscontrato che «*i cittadini non possono valersi della loro identificazione elettronica per autenticarsi in un altro stato membro perché i regimi nazionali di identificazione elettronica del loro paese non sono riconosciuti in altri Stati membri. Tale barriera elettronica impedisce ai prestatori di servizi di godere pienamente dei vantaggi del mercato interno*» (v. considerando 9).

In quest'ottica, il Regolamento ha l'obiettivo di promuovere la creazione di un *Digital Single Market* all'interno dell'Unione, rafforzando «*la fiducia nelle transazioni elettro-*

---

[3] Sul punto, cfr. C. LEONE, *EU Regulation no. 910/2014 on Electronic Identification and Trust Services: an effort towards the elimination of barriers for electronic transactions and internal market consolidation*, in *Riv. it. dir. pubb. comunit.*, 2015, p. 1048, secondo cui: «*The most relevant novelty of the Regulation is in the chosen legal instrument. It is, in fact, not a directive but a regulation, hence directly applicable to Member States without any transposition acts, as in the case of EU directives, whose aim is not harmonization and thus are to be considered as a law standardization instrument*»; nonché G. FINOCCHIARO, *Una prima lettura*, cit., p. 422, secondo cui: «*Non si tratta più di uno strumento di armonizzazione, ma invece di uno strumento di uniformazione del diritto per i ventotto Stati europei, eliminando così in radice quelle piccole differenze che rendono difficile realizzare compiutamente un mercato unico*».

[4] Cfr. J. ZILLER, *Diritto delle politiche e delle istituzioni dell'Unione europea*, Il Mulino, Bologna, 2013, p. 144 ss.; C. LEONE, *EU Regulation*, cit., p. 1049.

[5] V. Comunicazione della Commissione del 19 maggio 2010 "Agenda digitale europea" (*http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:it:PDF*) nella quale, preso atto della «*frammentazione dei mercati digitali*», della «*mancanza di interoperabilità*», dell'«*aumento della criminalità informatica e rischio di un calo della fiducia nelle reti*», della «*mancanza di investimenti nelle reti*», dell'«*impegno insufficiente nella ricerca e nell'innovazione*», della «*mancanza di alfabetizzazione digitale e competenze informatiche*» nonché delle «*opportunità mancate nella risposta ai problemi della società*» (cfr. *ivi*, p. 6 ss.), la Commissione ha individuato «*le azioni fondamentali basate sulla necessità di affrontare in modo sistematico queste sette aree problematiche*», al fine di «*compiere le azioni individuate come un insieme di programmi finalizzati a promuovere le prestazioni socioeconomiche dell'Europa*» (cfr. *ivi*, p. 7).

[6] Cfr. R. TITOMANLIO, *Considerazioni introduttive sul Sistema Pubblico per la gestione dell'Identità Digitale di cittadini (SPID)*, in *GiustAmm.*, 2015, n. 3.

*niche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'*eBusiness *e del commercio elettronico, nell'Unione europea*» (considerando 2), attraverso «*l'eliminazione delle barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri*» (considerando 12).

Nella consapevolezza da parte dell'Unione europea dell'importanza di uniformare anche le regole del mercato elettronico europeo, conferendo un grado di fiducia ai suoi operatori almeno pari a quello delle transazioni fisiche, il Regolamento eIDAS vuole assicurare il maggior grado di interoperabilità possibile tra i vari sistemi adottati nei Paesi membri, istituendo chiare regole e responsabilità e garantendo, in questo settore, un livello adeguato di certezza del diritto ed il riconoscimento reciproco dei servizi di identificazione elettronica. Ciò anche al fine di evitare quanto accaduto con l'abrogata Direttiva 1999/93/CE in materia di firme elettroniche, in relazione alla quale sono state riscontrate divergenze nelle discipline nazionali a causa delle differenti soluzioni attuative adottate dai singoli Stati membri, con conseguenti problemi di interoperabilità transfrontaliera.

In questa prospettiva, il Regolamento rinnova profondamente il quadro normativo europeo relativo alle transazioni elettroniche, precedentemente limitato alla sola disciplina della firma elettronica. Fino all'adozione della normativa in commento, infatti, nelle discipline giuridiche di settore era del tutto assente una regolamentazione transfrontaliera in tema di servizi fiduciari (e-*Trust Services*), come la creazione e la verifica di marche temporali e sigilli elettronici, servizi di posta elettronica certificata, nonché la creazione e la convalida di certificati per l'autenticazione dei siti *web*.

L'adozione di una disciplina uniforme dimostra che il legislatore europeo ha considerato definitivamente superati i dubbi manifestati in sede di adozione della Direttiva 1999/93/CE circa la desiderabilità e la efficacia di una disciplina comune a livello comunitario [7] e ritiene più adeguata una strategia regolatoria tesa all'uniformazione del diritto nel territorio dell'UE, fermo restando il principio di neutralità tecnologica.

Parte della dottrina aveva sollevato perplessità circa l'opportunità dell'armonizzazione di questo settore, ritenendola non necessaria o addirittura dannosa. In particolare, in una prospettiva di analisi economica del diritto, si era messo in evidenza come non fosse giustificabile un intervento normativo in assenza di un c.d. "*market failure*"; a tale considerazione si aggiungeva la constatazione che, già all'epoca, erano presenti sul mercato differenti offerte di servizi di crittografia e sottoscrizione digitale che avrebbero potuto imporsi sul mercato attraverso meccanismi *bottom up*. Inoltre, si segnalava un forte rischio di obsolescenza della disciplina regolamentare e di un'incidenza negativa di essa sull'innovazione tecnologica [8]. A ciò si sommava l'ovvia considerazione

[7] V. per un'indicazione delle voci critiche nel panorama internazionale: M. SIEMS, *The eu directive on electronic signatures: a worldwide model or a fruitless attempt to regulate the future?*, in *Int'l Rev. of Law, Computers & Technology*, vol. 16, 2002, p. 7 ss., pubblicato in versione successivamente aggiornata (2007) su *www.ssrn.com* (da cui si cita).

[8] Più precisamente, la direttiva si basava principalmente sul sistema di chiavi a crittografia pubblica, mentre altre istituzioni, come ad es. UNCITRAL (v. *Model law on electronic signatures*, disponibile su *https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf*) e OECD (OECD *Re-*

dell'inidoneità di una disciplina regionale ad avere un impatto a livello globale.

Si tratta, invero, di rilievi che erano già a suo tempo superabili nella misura in cui l'obiettivo della direttiva era circoscritto alla difficilmente controvertibile esigenza di fornire un adeguato livello di certezza a determinate transazioni elettroniche, principalmente nei settori in cui vi era un siffatto peculiare bisogno [9]. Non sorprende che la Commissione rilevasse nel 2006 che i servizi di firma elettronica erano diffusi quasi unicamente nel settore bancario e nei rapporti tra cittadino e P.A. [10]. Ciò ha spinto una parte degli autori a ravvisare un vero e proprio fallimento degli scopi della direttiva, motivato con le difficoltà di introdurre un capillare uso della crittografia per il consumatore medio dei servizi *on line* [11].

Del resto, anche la dottrina italiana ha correttamente segnalato, più in generale, che anche nel Regolamento eIDAS il legislatore ha valutato il problema dell'accertamento dell'identità *on line* nella specifica prospettiva di quei servizi che richiedono un elevato livello di certezza nell'eseguire tale verifica, come i servizi bancari e quelli pubblici [12]. In altri termini, è il caso di rimarcare che il regolamento non intende fornire una risposta normativa alla questione più ampia e complessa della tutela del diritto all'identità *on line* con particolare riferimento ai meccanismi di c.d. "*soft ID*", sempre più diffusi in rete [13].

---

commendation on Electronic Authentication and OECD Guidance for Electronic Authentication, *https://www.oecd.org/sti/ieconomy/38921342.pdf*), mantenevano un approccio più neutrale dal punto di vista tecnologico.

[9] V. M. SIEMS, *The eu directive on electronic signatures*, cit., p. 23 s.

[10] Cfr. Relazione della Commissione al Parlamento europeo e al Consiglio del 15 marzo 2006, intitolata "*Relazione sull'attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*", in cui si legge quanto segue: «*Le due applicazioni dominanti sono connesse ai servizi di* egovernment *e di* personal ebanking*. Molti Stati membri e numerosi altri paesi europei hanno varato, o intendono varare, applicazioni egovernment, applicazioni che sovente si basano sull'uso di carte di identità elettroniche. Queste possono essere utilizzate sia come documenti di identità che per consentire l'accesso in linea ai servizi pubblici rivolti ai cittadini. Nella maggior parte dei casi queste carte di identità contengono le tre funzionalità: identificazione, autenticazione e firma. L'altra grande applicazione della firma elettronica – il* personal ebanking *– si trova ormai in fase di decollo nella maggior parte dei paesi dell'UE. La maggioranza dei sistemi di autenticazione per questo tipo di servizi si basa su simboli e password monouso, cioè su quella che la direttiva designa come la forma più semplice di firma elettronica. Sebbene molte applicazioni di* ebanking *utilizzino queste tecnologie soltanto a fini di autenticazione dell'utente, è anche in aumento il ricorso alla firma elettronica delle transazioni bancarie. Per i servizi di* ebanking *rivolti alle imprese (*business-to-business*) e di compensazione interbancaria è più comune l'utilizzo delle smart card, che si ritiene offrano un più elevato livello di sicurezza*».

[11] T.Z. ZARSKY-N.N. GOMES DE ANDRADE, *Regulating electronic identity intermediaries: the soft eID conundrum*, in 74 *Ohio St. L.J.*, (2013), pp. 1336 ss., 1382.

[12] V. G. FINOCCHIARO, *Una prima lettura*, cit., p. 419. Sul punto, v. anche il considerando 12, ove uno specifico riferimento all'obiettivo di rimuovere le barriere «*almeno per l'autenticazione nei servizi pubblici*» e il considerando 17 ove è espresso l'auspicio che gli Stati membri «*incoraggino il settore privato a impiegare volontariamente mezzi di identificazione elettronica nell'ambito di un regime notificato a fini di identificazione ove necessario*».

[13] Cfr. T.Z. ZARSKY-GOMES DE ANDRADE, *Regulating electronic identity intermediaries*, cit., p. 1336 ss., v. in part. p. 1383. In generale sul tema dell'identità digitale: v. N.N. GOMES DE ANDRADE,

Il legislatore europeo ha così scelto di uniformare, mantenendo un approccio tecnologicamente neutrale, alcuni strumenti atti ad assicurare l'effettività del mercato digitale transfrontaliero all'interno dell'Unione europea, come ad es. la gestione delle identità elettroniche, l'utilizzo di strumenti atti a garantire la veridicità di un sito Internet, i sistemi di posta elettronica in grado di fornire ricevute di consegna al mittente, una nuova disciplina delle firme elettroniche e l'introduzione dei sigilli elettronici, ed i servizi di marcatura temporale [14].

Il Regolamento «*non intende intervenire riguardo ai sistemi di gestione dell'identità elettronica e relative infrastrutture istituiti negli Stati membri*» (considerando 12), ma solo fornire alcune indicazioni minime di sicurezza per garantire l'interoperabilità tra i differenti sistemi sviluppati negli Stati membri [15], là dove siano richiesti dall'erogatore del servizio pubblico livelli di garanzia elevati nell'accesso al servizio [16].

2. Oggetto della nuova disciplina. a) L'identificazione elettronica

L'art. 1 del Regolamento individua l'oggetto della disciplina introdotta dal Regolamento eIDAS.

In particolare, tale previsione dispone che «*allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari*» il regolamento: (*i*) «*fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro*» (lett. a); (*ii*) «*stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche*» (lett. b); (*iii*) «*istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web*» (lett. c).

Prendendo le mosse dall'identificazione elettronica (*electronic identification*), essa è definita dal regolamento come «*il processo per cui si fa uso di dati di identificazione*

Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, in *Computers, Privacy and Data Protection: An Element of Choice*, S. Gutwirth, Y. Poullet, P. De Hert and R. Leenes (eds.), Springer (2011), p. 65; G. PINO, *The right to personal identity in Italian private law: constitutional interpretation and judge-made rights*, in *The harmonisation of European private law*, Van Hoecke-Ost eds., Hart Publishing, Oxford, 2000, p. 225 ss.; per ulteriori riferimenti v. G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Dig. disc. priv., sez. civ.*, Agg., Torino, 2010, p. 720 ss.; G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, p. 511 ss.

[14] Vale la pena chiarire che molti degli strumenti appena citati sono già in uso nell'ordinamento italiano, e regolati nel Codice dell'Amministrazione digitale e nelle norme attuative emanate dall'Agenzia per l'Italia Digitale; altri invece costituiscono un'innovazione per il sistema italiano.

[15] V. considerando 14.

[16] V. considerando 15, ove è espressamente riconosciuta la libertà degli Stati membri «*di riconoscere mezzi di identificazione elettronica aventi livelli di garanzia dell'identità inferiori*».

personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica» (art. 3, par. 1), e si distingue dalla «*autenticazione elettronica*» che è invece individuata come il «*processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica*» (art. 3, par. 5) [17].

In relazione ai sistemi di identificazione elettronica, il Regolamento prevede che ciascuno Stato membro possa notificare i sistemi di identificazione elettronica forniti ai cittadini e alle aziende ai fini del mutuo riconoscimento, lasciando così impregiudicata la libertà degli Stati membri di stabilire quali strumenti di identificazione elettronica utilizzare per l'accesso ai servizi *on line* all'interno del proprio territorio [18].

In quest'ottica, ben si comprende l'obbligo di assicurare il mutuo riconoscimento dei mezzi di identificazione elettronica rilasciati in un altro Stato membro per accedere a un servizio pubblico *on line*, a condizione che tali mezzi di identificazione rientrino in un regime di identificazione elettronica notificato alla Commissione e siano soddisfatte le condizioni relative a livelli di garanzia richiesti. Ne risulta che poiché non è richiesta l'adozione di uno strumento di identificazione *on line* condiviso, ciascuno Stato membro può mantenere gli strumenti di identificazione *on line* già operanti [19], ma è tenuto a riconoscere [20] ogni sistema di identificazione notificato da altri Stati membri che abbiano un livello di sicurezza pari o superiore a quello del servizio offerto (e sempre che tale livello di sicurezza sia almeno "sostanziale" o "elevato") [21].

Volendo fornire una schematizzazione, il Regolamento disegna un sistema connotato da un rapporto trilaterale al cui apice è situato l'organismo di vigilanza pubblico (art.

---

[17] Si noti, peraltro, che nell'ordinamento italiano, e più esattamente nel Codice dell'Amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), l'identificazione informatica è definita come «*la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso*» (art. 1, co. 1, lett. u-*ter*). L'autenticazione, invece, non si riferisce più al soggetto che accede al sistema informatico, ma al documento informatico. Essa consiste nella «*validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione*» (art. 1, co. 1, lett. b). Una definizione più generale di autenticazione informatica è poi contenuta all'interno del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196, art. 4, co. 3, lett. c), ove è definita come «*l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità*».

[18] V. considerando 13.

[19] In questi termini, cfr. G. FINOCCHIARO, *Una prima lettura*, cit., p. 423. V. anche considerando 12, 13.

[20] Il regolamento opportunamente prevede che sia garantita l'interoperabilità tecnica dei sistemi di identificazione notificati.

[21] Va precisato che, mentre per il settore pubblico, il riconoscimento dei sistemi di identificazione notificati è un obbligo, per i privati si tratta di una facoltà: v. G. FINOCCHIARO, *Una prima lettura*, cit., p. 424, la quale riconosce che «*il settore privato avrà ogni interesse ad estendere il proprio mercato, avvalendosi di servizi di identificazione on line*».

17 Reg. eIDAS), mentre ai lati si collocano i prestatori di servizi fiduciari, i quali garantiscono l'integrità e la correttezza del funzionamento dei sistemi di identificazione digitale, e le persone fisiche e giuridiche, che utilizzano tali servizi [22]. In Italia, il ruolo apicale è stato attribuito all'Agenzia per l'Italia Digitale (AgID) [23] e, in tale ambito, si segnala l'istituzione del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID), introdotto con d.p.c.m. 24 ottobre 2014 e pubblicato in Gazzetta Ufficiale il 9 dicembre 2014, che rappresenta un'espressa attuazione a livello nazionale del regolamento eIDAS [24].

Poiché non è possibile in questa sede provvedere a un'analisi della disciplina regolamentare in materia di identità digitale, ci si limita qui a evidenziare che attraverso l'introduzione della disciplina in tema di SPID è stato inaugurato nel nostro Paese un nuovo sistema di identificazione elettronica con caratteristiche adeguate, affinché il suo utilizzo sia possibile anche al di fuori del territorio italiano, e grazie al quale pubbliche amministrazioni e imprese private possono consentire di accedere ai propri servizi a cittadini e imprese attraverso un'unica identità digitale.

Va poi tenuto in conto che il decreto SPID rappresenta il primo esempio a livello europeo di attuazione del Regolamento eIDAS, realizzando l'intento del legislatore europeo di voler incoraggiare anche nel settore privato l'utilizzo dei mezzi di identificazione elettronica a fini di identificazione [25].

Una conferma in questa direzione si può rinvenire nelle recenti modifiche apportate dal d.lgs. 26 agosto 2016, n. 179 al Codice dell'Amministrazione Digitale, tra le quali si evidenziano l'inserimento di una nuova definizione di "identità digitale" (art. 1, co. 1, lett. u-*quater*), qualificata come la «*rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64*» (con espresso richiamo, dunque, al decreto SPID) [26]; nonché la previsione all'art. 3 del "diritto" per tutti i cittadini e le imprese di possedere una propria "identità digitale", operando un evidente riferimento al sistema SPID che acquisi-

---

[22] Così C. LEONE, *EU Regulation*, cit., p. 1046.

[23] Istituita dall'art. 19 del d.l. 9 febbraio 2012, n. 5 (c.d. decreto crescita) conv. con modifiche dalla legge 4 aprile 2012, n. 35.

[24] Del resto, nello stesso preambolo del d.p.c.m. 24 ottobre 2014 si legge: «*Visto il 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, pubblicato nella Gazzetta Ufficiale dell'Unione Europea – serie L 257 del 28 agosto 2014*»; in argomento, cfr. R. TITOMANLIO, *Considerazioni introduttive*, cit.

[25] Al riguardo si segnala che lo Stato italiano ha anche già provveduto a notificare alla Commissione il decreto SPID e conseguentemente, come previsto dal Regolamento eIDAS, dal 1° luglio 2016, lo SPID dovrà essere riconosciuto e accettato da tutti gli altri stati membri dell'Unione.

[26] Merita in proposito ricordare che prima di tali modifiche la definizione di «identità digitale» era prevista dall'art. 1, comma 1, lett. o) del decreto SPID come «*la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi*». Sul punto v. C. LEONE, *EU Regulation*, cit., p. 1055.

sce così un ruolo centrale nell'accesso da parte dei cittadini ai servizi *on-line* della pubblica amministrazione e a quelli erogati dagli operatori privati che vi aderiranno [27].

3. b) I servizi fiduciari

Secondo quanto previsto dalla lett. b) dell'art. 1 in esame, il Regolamento stabilisce «*le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche*».

Al riguardo va anzitutto premesso che la locuzione "servizio fiduciario" (o *trust service*) indica «*un servizio elettronico fornito normalmente dietro remunerazione*», caratterizzato dalla «*creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi*», dalla «*creazione, verifica e convalida di certificati di autenticazione di siti web*», nonché dalla «*conservazione di firme, sigilli o certificati elettronici relativi a tali servizi*» (art. 3, par. 1, n. 16).

Si tratta, a prima vista, di una definizione piuttosto ampia che comprende molti dei servizi offerti sul mercato [28]. Come si è notato, rispetto alla Direttiva 1999/93/CE, il Regolamento innova il quadro normativo, disciplinando in modo uniforme la prestazione di servizi ulteriori rispetto alla sola creazione, verifica e convalida delle firme elettroniche.

Il legislatore europeo non ha ritenuto opportuno istituire un obbligo generale di ciascun prestatore di servizi fiduciari di adeguarsi alla disciplina di nuova introduzione (considerando 21), ma ha opportunamente distinto i servizi qualificati, soggetti alla penetrante disciplina del regolamento, da quelli non qualificati, che sono disciplinati solo riguardo ad alcuni aspetti. Più precisamente, l'art. 3, par. 1, n. 17 definisce «*qualificato*» un servizio fiduciario che soddisfa determinati requisiti stabiliti dal regolamento eIDAS e fornisce quindi garanzie superiori in termini di sicurezza e qualità del servizio. Inoltre, i servizi qualificati sono sottoposti alla vigilanza di un apposito organismo nazionale, (in Italia, l'Agenzia per l'Italia Digitale) secondo quanto stabilito nel Capo III del Regolamento [29] (v., in part., artt. 17 e 20) e sono soggetti all'iscrizione in un apposito albo (c.d. "elenco di fiducia", art. 22).

Il Regolamento stabilisce le condizioni per l'avvio di un servizio fiduciario qualificato (art. 21) e i requisiti da rispettare quando il prestatore rilascia un certificato qualificato per un servizio fiduciario (art. 24). Viene altresì regolato (art. 11) il regime della responsabilità nonché l'onere della prova per i danni causati in seguito al mancato adempimento da parte dei prestatori di servizi fiduciari degli obblighi previsti nello stesso regolamento. Una volta autorizzato e iscritto all'albo il prestatore di servizi fidu-

---

[27] Sul punto, cfr. il documento del Consiglio Nazionale del Notariato in data 3 ottobre 2016, dal titolo "*Le modifiche al codice dell'amministrazione digitale. Commento alle novità di interesse notarile*", p. 12.

[28] Cfr. G. FINOCCHIARO, *Una prima lettura*, cit., p. 426.

[29] Si noti, peraltro, che il concetto di servizio fiduciario qualificato ricomprende i certificatori accreditati (che rilasciano le *smart card* per la firma digitale), i conservatori accreditati e gestori di posta elettronica certificata già presenti in Italia.

ciari qualificati è autorizzato a utilizzare il c.d. "Marchio di fiducia UE" (art. 23), ossia un segno distintivo assegnato al prestatore per incrementare la fiducia degli utenti nei servizi *on line* e segnalare al mercato le garanzie offerte in relazione a quel determinato servizio fiduciario (considerando 47).

Per contro, i servizi fiduciari non qualificati sono oggetto di una scarna disciplina riguardante la loro responsabilità (art. 13), l'accessibilità da parte di persone disabili (art. 15), ma sono comunque soggetti a più limitate forme di vigilanza da parte dell'organismo designato da ciascuno Stato membro (art. 17), al fine di garantire la diligenza, la trasparenza e l'attendibilità dei servizi prestati (considerando 35 e 36). È invece riservata al legislatore nazionale la disciplina di profili non considerati dal Regolamento con riferimento ai servizi fiduciari non qualificati.

Va notato, tuttavia, che sussistono alcune differenze di rilievo rispetto al regime previsto dalla normativa previgente (Direttiva europea 1999/93/EC).

Sotto un primo profilo, il concetto di "accreditamento" è stato sostituito da quello di "qualificazione", verosimilmente al fine di non creare confusione con il tema degli «*obblighi in materia di accreditamento degli organismi di valutazione della conformità e vigilanza del mercato di prodotti*» (considerando 44), regolato da procedure definite a livello internazionale e svolto da un ente di accreditamento riconosciuto.

Sotto altro profilo, si assiste all'ampliamento della figura del "prestatore di servizi di certificazione" che è stata sostituita da quella del "prestatore di servizi fiduciari" definito all'art. 3, par. 19, come «*una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato*». Ne deriva che il certificatore accreditato per la firma qualificata diventa un prestatore di servizi fiduciari qualificato per la sottoscrizione elettronica.

Si consideri, in aggiunta, che oltre alla già prevista funzione di vigilanza, che risulta confermata anche alla luce della nuova disciplina, il legislatore europeo ha introdotto la obbligatoria sottoposizione dei prestatori di servizi fiduciari a valutazioni di conformità da parte di idonei soggetti terzi [30] (cfr. art. 20), i quali devono essere a loro volta accreditati da un apposito ente riconosciuto [31].

Occorre, infine, segnalare alcune incertezze che ha generato in Italia l'attuazione

---

[30] In particolare, l'"organismo di valutazione della conformità" è qualificato all'art. 3, par. 18, come «*un organismo ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati*».

[31] Ciò significa che i soggetti che prestano servizi fiduciari qualificati sono sottoposti sia a valutazione di conformità da parte di un ente terzo accreditato o organo europeo equivalente, sulla base di requisiti che saranno indicati dalla Commissione mediante appositi atti esecutivi; sia alla vigilanza di un organismo di vigilanza (l'AgID per l'Italia), il quale, sulla base del certificato rilasciato in seguito alla valutazione di conformità, provvede o meno a confermare la qualificazione attribuita. A parte ciò, e in generale, il Regolamento amplia il novero dei possibili servizi, includendo, ad esempio, i servizi per la creazione e verifica delle firme elettroniche, nell'ambito dei quali, in linea di principio, dovrebbero essere ricompresi i servizi di firma in mobilità o da remoto, il cui ruolo decisivo ai fini della diffusione delle tecnologie regolate dalla nuova disciplina è riconosciuto dallo stesso Regolamento.