In vigore dal 17 settembre 2014, il regolamento c.d. "eIDAS" (*electronic IDentification Authentication and Signature*), reca le condizioni per il riconoscimento reciproco in ambito di identificazione elettronica e le regole comuni per le firme elettroniche, l'autenticazione web ed i relativi servizi fiduciari per le transazioni elettroniche. Opportunità e rischi per l'Italia.

di Daniele TUMIETTO e Andrea CACCIA

REGOLAMENTO EUROPEO EIDAS

***Daniele TUMIETTO**, commercialista, è titolare dell'omonimo Studio Tributario, componente del Forum Italiano della Fattura Elettronica presso l'Agenzia delle Entrate, commercialista Partner di Menocarta.net e socio fondatore di Menocarta.pro, collaboratore degli Osservatori della School of Management del Politecnico di Milano per le problematiche connesse alla conservazione sostitutiva e alla fatturazione elettronica all'interno delle aziende e degli studi professionali, componente del comitato di coordinamento di ABIRT (Advisory Board Italiano dei Responsabili del Trattamento dei dati personali) e di ISOC – Internet Society.*

***Andrea CACCIA,** ingegnere, si occupa di dematerializzazione e delle relative tecnologie: standard e compliance tecnico-normativa di firma, identità, fatturazione, trasmissione e conservazione elettronica dei documenti. Su queste tematiche è coinvolto nelle attività di normazione tecnica (standard) a livello nazionale (UNI/UNINFO), europea (CEN/ETSI) e internazionale (ISO, OASIS, UN/CEFACT).*

Con l'adozione del Regolamento (UE) n. 910 del 23 luglio 2014 (2014/910/UE) "eIDAS" il quadro normativo definito dalla Direttiva Europea 1999/93/EC sulle firme elettroniche e dalle relative leggi nazionali di recepimento è ormai prossimo ad un fondamentale aggiornamento su scala europea, volto a garantire la piena interoperabilità a livello comunitario non solo della firma elettronica ma di tutto un insieme di servizi di terza parte detti fiduciari (traduzione dell'inglese Trust Service provider) e di servizi di identificazione ed autenticazione.

Il Regolamento, entrato in vigore il 17 settembre 2014, troverà applicazione gradualmente nel corso dei prossimi mesi e, in particolare, dal 1 luglio 2016 con l'abrogazione della Direttiva 1999/93/EC, fatti salvi certificati, firme e dispositivi preesistenti, superando ogni norma in contrasto a livello nazionale che viene ad essere implicitamente abrogata. Un Regolamento europeo è, infatti, una norma di legge che, in base alle regole comunitarie, è direttamente applicabile senza necessità di ulteriori passaggi a livello dei singoli Stati membri che garantisce, pertanto, una uniformità di applicazione in tutto il territorio dell'Unione.

L'entrata in vigore del Regolamento rivoluziona fortemente il quadro normativo vigente (Figura 1), sia in Italia che negli altri Stati membri, centralizzando anche l'emissione degli atti di esecuzione, che dovranno richiamare sempre, con l'eccezione di pochi casi specifici, le norme degli enti di standardizzazione il cui uso in passato è sempre stato discrezionale, minando così gravemente la possibilità di garantire l'interoperabilità.

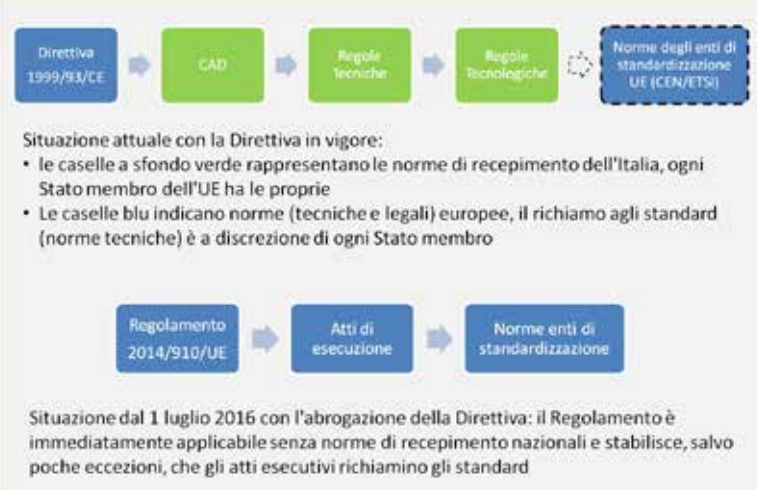

***Figura 1** – Quadro normativo vigente.*

Questo Regolamento crea un nuovo contesto giuridico e tecnico fondato sul principio di neutralità tecnologica che, grazie all'uso di strumenti di legislazione secondaria, consente sia di individuare in modo preciso il quadro di *standard* di riferimento per garantire l'interoperabilità sia di poter aggiornare tale quadro in modo flessibile per adattarlo alle nuove tecnologie. Gli *standard* comuni consentono lo sviluppo di servizi fiduciari digitali che garantiscono un livello di affidabilità uniforme nell'Unione e di promuovere così la fiducia nelle transazioni elettroniche favorendo la creazione ed il successo del mercato digitale unico europeo.

La nuova normativa si occupa, sia nel pubblico che nel privato, di identità, firme, sigilli, validazioni temporali e documenti elettronici, servizi di recapito elettronico, servizi di autenticazione e certificazione dei siti *web* e più in generale di tutti i servizi digitali in cui è essenziale la fiducia nella controparte.

Appare immediatamente chiaro, in un contesto di sempre maggiore diffusione del digitale nei processi aziendali e della pubblica amministrazione, l'esigenza di avere garanzie chiare sull'identificazione delle controparti, sul valore legale dei documenti e della relativa trasmissione e, in generale, dei servizi digitali resi disponibili.

Identificazione e autenticazione elettronica

L'**identificazione elettronica** indica il processo in cui si usano i dati di autenticazione personale in forma elettronica che rappresentano univocamente una persona fisica o una persona legale o una persona fisica che rappresenti una persona legale, ad esempio per accedere a servizi *online*. L'**autenticazione elettronica** è il processo elettronico che consente di confermare l'identificazione elettronica o l'origine e l'integrità di dati in forma elettronica. L'istituzione del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID) è un sistema italiano che nasce con ambizioni europee con il quale le pubbliche amministrazioni e i privati potranno consentire l'accesso in rete ai propri servizi.

Il Regolamento istituisce un regime di mutuo riconoscimento delle identità elettroniche europee e si auspica che SPID possa avere le caratteristiche adeguate perché il suo utilizzo sia possibile anche al di fuori del territorio italiano.

Firma elettronica

La firma elettronica rappresenta un insieme di dati che sono allegati o connessi, mediante una associazione logica, ad altri dati elettronici e sono utilizzati da una persona fisica per sottoscrivere elettronicamente un documento, e si distingue in:

Firma Elettronica Avanzata (FEA), avente le seguenti caratteristiche:

- è connessa unicamente al firmatario,
- è idonea ad identificare il firmatario,
- è creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo,
- è collegata ai dati sottoscritti mediante una connessione che permette di rilevare qualsiasi successiva modifica dei predetti dati;

Firma Elettronica Qualificata (FEQ), che possiede queste caratteristiche, in aggiunta a quelle di una Firma Elettronica Avanzata:

- è creata da un dispositivo qualificato per la creazione di una firma elettronica,
- è basata su un certificato elettronico qualificato.

Le definizioni sono molto simili a quelle contenute nella Direttiva 1999/93/EC sulle firme elettroniche attualmente in vigore, introducendo però la definizione precisa di FEQ, che non era stata formulata in modo specifico.

Sigillo elettronico

Il Sigillo Elettronico è una novità: simile alla firma elettronica ma apposta da una persona giuridica, serve a garantire l'origine e l'integrità dei dati ad esso associati. Anche per il sigillo elettronico vi sono le definizioni di **Sigillo Elettronico Avanzato** e di **Sigillo Elettronico Qualificato**. Al sigillo elettronico, anche avanzato, non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali qualora non soddisfacesse i requisiti del sigillo elettronico qualificato. Un sigillo elettronico qualificato gode della presunzione legale (inversione dell'onere della prova) di integrità e provenienza dei dati cui il sigillo elettronico qualificato è associato.

Servizi fiduciari (Trusted Services)

Con il termine **servizio fiduciario** si indica un insieme di servizi elettronici, forniti in genere a pagamento, caratterizzati come segue:

- creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati relativi a tali servizi;
- creazione, verifica e convalida di certificati di autenticazione di siti *web*;
- conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Un servizio fiduciario che soddisfa determinati requisiti stabiliti dal Regolamento eIDAS e fornisce garanzie superiori in termini di sicurezza e qualità del servizio viene detto "qualificato" ed è sottoposto a vigilanza da un apposito organismo nazionale (l'Agenzia per l'Italia Digitale in Italia) secondo quanto stabilito nella Sezione 2 nel Regolamento.

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. Ci sono però alcune differenze importanti rispetto al regime vigente basato sulla Direttiva Europea 1999/93/EC. Innanzi tutto il termine "accreditamento" è stato sostituito da "qualificazione" per non creare confusione con l'accreditamento degli organismi di certificazione di prodotti, servizi, sistemi di gestione e qualificazioni professionali, che avviene secondo schemi definiti a livello internazionale e che è svolto da un ente di accreditamento riconosciuto (in Italia si tratta di Accredia). Oltre alla precedente funzione di vigilanza, che resta anche nel nuovo regime, si introduce l'obbligo per i prestatori di servizi fiduciari di essere sottoposti a valutazioni di conformità da parte di idonei soggetti terzi che devono essere accreditati da un ente di accreditamento riconosciuto. In pratica, ogni soggetto che presta servizi fiduciari qualificati è sottoposto sia a valutazione di conformità da parte di un ente terzo accreditato da Accredia o organo europeo equivalente, sulla base di requisiti definiti da standard che saranno indicati dalla Commissione mediante appositi atti esecutivi, sia alla vigilanza di un organismo di vigilanza, l'AgID per l'Italia, che sulla base del certificato rilasciato a seguito della valutazione di conformità, potrà confermare o meno la qualificazione. Il Regolamento, inoltre, estende l'ambito dei possibili servizi, includendo, ad esempio, servizi per la creazione e verifica delle firme elettroniche, dove presumibilmente ricadranno servizi di firma in mobilità o anche remota, il cui ruolo decisivo per la diffusione di queste tecnologie, è riconosciuto dal Regolamento.

Vigilanza e requisiti dei servizi fiduciari

Il Regolamento eIDAS, a differenza della Direttiva, indica in modo puntuale all'art. 17 i compiti degli organismi di vigilanza, uno per Stato membro, e le modalità di mutua assistenza (art. 18) con l'intento di stabilire, grazie alla cooperazione tra questi organismi, un quadro di riferimento per la vigilanza il più possibile uniforme sul territorio dell'Unione.

La vigilanza avviene *ex ante* per i prestatori di servizi fiduciari qualificati, *ex post* per tutti, inclusi pertanto i prestatori non qualificati.

All'articolo 19 sono indicati i requisiti di sicurezza e gli obblighi per tutti i prestatori di servizi fiduciari:

- l'adozione di misure tecniche e organizzative opportune per gestire i rischi sulla sicurezza dei servizi offerti e di misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti;
- l'obbligo di notificare all'organismo di vigilanza appena possibile, comunque entro 24 ore dal rilevamento, le violazioni di sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari forniti, o sui dati personali custoditi;
- nel caso in cui vi sia la probabilità che una violazione della sicurezza o perdita di integrità abbia effetti negativi su una persona fisica o

giuridica, occorre notificare la violazione o la perdita anche a quest'ultima;
- quando la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza che riceve la notifica informa quelli degli altri Stati membri interessati e l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA);
- l'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico;
- l'organismo di vigilanza trasmette all'ENISA annualmente una sintesi delle notifiche di violazione pervenute dai fornitori di servizi fiduciari.

All'articolo 21 sono descritte le modalità di avvio delle attività dei prestatori di servizi fiduciari:
- i prestatori di servizi fiduciari che ancora non posseggono la qualifica notificano all'organismo di vigilanza (*supervisory body*) la loro intenzione di fornire servizi qualificati fornendo contestualmente una relazione di valutazione della conformità (*conformity assessment report*) rilasciata da un organismo di valutazione della conformità accreditato (*conformity assessment body*), che è il risultato di una valutazione periodica da fare almeno ogni 24 mesi (art. 16);
- l'organismo di vigilanza verifica che il prestatore di servizi fiduciari ed i servizi da lui offerti soddisfino i requisiti previsti del Regolamento.

In caso di verifica con esito positivo:
- viene concesso lo status di "qualificato" al prestatore e ai suoi servizi offerti;
- viene effettuato l'aggiornamento della lista di fiducia (*trusted list*) oppure, ove l'organismo gestore della lista non coincida con l'organismo di vigilanza, viene richiesto di aggiornare la lista;
- dal momento in cui il prestatore ha ricevuto lo status di qualificato, esso può cominciare ad offrire liberamente servizi fiduciari qualificati.

Appare rilevante ora andare ad esaminare l'articolo 23, che disciplina il marchio di fiducia UE per i servizi fiduciari qualificati. Come sopra indicato, i fornitori di servizi fiduciari qualificati, quando sono riconosciuti come tali e quindi inseriti nelle liste di fiducia, possono usare il marchio di fiducia UE per indicare che i servizi fiduciari forniti sono qualificati (*Trustmark*).
Tale marchio, definito dalla Commissione Europea, potrà essere pubblicato sul sito web del fornitore, con un *link* alla lista di fiducia nazionale per permettere a ciascun utilizzatore del servizio di verificare il reale inserimento nella lista di fiducia.

Nel seguente articolo 24 sono indicate le regole aggiuntive per i prestatori di servizi fiduciari qualificati. Un prestatore di servizi fiduciari che emette un certificato qualificato per un servizio fiduciario deve verificare in modo opportuno l'identità della persona fisica o giuridica, direttamente o ricorrendo ad un terzo in conformità della normativa nazionale, mediante:
- presenza *de visu* della persona fisica o rappresentante autorizzato della persona giuridica al momento della richiesta;
- mezzi di identificazione elettronica a distanza mediante mezzi per il cui rilascio è stata richiesta la presenza *de visu* della persona fisica o rappresentante autorizzato e che rispondono a livelli di garanzia alto o sostanziale, con riferimento all'articolo 8;
- mediante utilizzo di un certificato di una Firma Elettronica Qualificata o un Sigillo Elettronico Qualificato;
- con altri mezzi, riconosciuti a livello nazionale, che forniscono una garanzia equivalente alla presenza fisica.

Gli obblighi dei fornitori di servizi fiduciari qualificati sono i seguenti:
- informare l'organismo di vigilanza sulle variazioni e cessazione della propria attività;
- utilizzare ed impiegare personale e, ove presenti, subcontraenti che siano competenti e formati in materia di norme di sicurezza e protezione dei dati personali, utilizzando procedure conformi alle norme europee o internazionali;
- mantenere risorse finanziarie adeguate e/o stipulare un'adeguata assicurazione per la responsabilità civile sui danni;
- fornire un'informazione chiara e completa agli utilizzatori sulle condizioni esatte e sulle eventuali limitazioni di utilizzo dei servizi;
- usare sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi da essi gestiti;
- utilizzare sistemi affidabili per memorizzare i dati gestiti che garantiscano l'autenticità dei dati e il controllo degli accessi a tali dati;
- adottare misure adeguate contro le falsificazioni e il furto dei dati;
- registrare, anche in forma elettronica, l'accesso a tutti i dati rilasciati e ricevuti. Le registrazioni e le informazioni relative, per un congruo periodo di tempo, devono essere conservate anche dopo la cessazione delle attività;
- definire ed aggiornare un piano di cessazione delle attività per garantire la continuità del servizio a beneficio dei clienti;
- effettuare il trattamento lecito dei dati personali a norma della Direttiva 95/46/CE;
- i fornitori di servizi fiduciari che rilasciano certificati qualificati devono istituire una banca dati dei certificati e mantenerla aggiornata.

Conclusioni

Il Regolamento eIDAS rappresenta un passo avanti importante verso l'obiettivo del Mercato unico digitale, con l'ambizione di costruire un quadro di riferimento sicuro ed interoperabile per le transazioni elettroniche. Trattandosi di un Regolamento, la sua entrata in vigore non è soggetta a recepimento, questo garantisce regole certe ed uniformi su tutto il territorio dell'Unione ma, ove le norme preesistenti non venissero allineate, eliminando tutte quelle parti che sarebbero soggette ad abrogazione implicita e creando i raccordi con la nuova normativa, si arriverebbe inevitabilmente ad una situazione di sicura confusione che danneggerebbe operatori ed utilizzatori. Per l'Italia, Paese leader internazionale su queste tematiche, il Regolamento eIDAS rappresenta quindi un'opportunità ed un rischio: l'opportunità è chiaramente quella di un mercato molto più ampio per le imprese nazionali che la sapranno cogliere e si apriranno ai mercati esteri; il rischio è legato non solo alla scarsa propensione di molte piccole e medie imprese italiane ad operare sui mercati esteri, ma anche a quello di non riuscire a dotarsi per tempo di un nuovo quadro normativo che tenga conto di queste importanti novità. ©