KnowIT

Rivista scientifica per i manager della governance digitale e della privacy

FEA, biometria, privacy e compliance: il nuovo scenario europeo

Atti del Convegno AIFAG - Lecce, 24 giugno 2016

Indice

KnowIT. Rivista scientifica trimestrale gratuita per i manager della governance digitale e della privacy.

Anno 1 - Numero 0 - Settembre 2016 - Testata iscritta al n. 6/2016 del Registro della Stampa del Tribunale di Lecce il 23 maggio 2016, ISSN (in fase di attribuzione)

Direttore responsabile: Silvia Riezzo

Direttore editoriale: Andrea Lisi

Editore: KnowIT è pubblicata da Clio S.p.A. Via 95° Rgt. Fanteria n°70 - 73100 Lecce. Tel. +39 0832 344041 - Fax +39 0832 340228
www.clio.it - info@clio.it

EDITORIALE: Il dovere di formarsi nonostante tutto ciò che accade intorno

Avv. Andrea Lisi - *Direttore Editoriale, Presidente ANORC Professioni*

Mentre la canicola estiva cede il passo a temperature più miti, ci troviamo a riprendere in mano anche le fila (alcune purtroppo particolarmente sfilacciate) dei processi di innovazione digitale nel nostro Paese: dove eravamo rimasti?

Settembre è il mese che dopo l'estate porta il dono usato della perplessità: così diceva in una canzone di qualche anno fa un noto cantautore che non ci sentiamo di contraddire, anzi, semmai potremmo aggiustare un po' il tiro specificando che, in quest'estate più che in altre, la perplessità è stata una nostra costante compagna.

Vera e propria incredulità è stata quella che abbiamo provato, infatti, la prima settimana di agosto **alla notizia del parere favorevole reso dalla Commissione Affari Costituzionali al Decreto Legislativo che modifica il CAD, parere che, proprio alle soglie dell'importante scadenza del 12 agosto, entro la quale le Pubbliche Amministrazioni inadempienti avrebbero dovuto senza più scuse adeguarsi alle regole tecniche** in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, con incredibile nonchalance **ha richiesto al Governo di sospendere l'efficacia di queste ultime a tempo indefinito**, in attesa che vengano emanate delle nuove regole tecniche "pienamente conformi alle disposizioni del Codice" (le regole vigenti in materia di formazione del documento informatico, vale la pena ricordarlo, erano entrate in vigore nel nostro ordinamento solo poco più di un anno fa…).

Questo *coup de théâtre* sembrava rispondere a uno schema fin troppo diffuso nell'agire italico, quello dei tre passi avanti e due indietro. La previsione di sospendere l'applicazione delle citate regole tecniche rischiava, infatti, di mettere in crisi quel poco di buono che tante PA in modo coraggioso avevano realizzato sino ad oggi in materia di digitalizzazione dei propri documenti (proprio osservando le utili indicazioni contenute nel DPCM che si intendeva "sospendere"). **Le copiose critiche sopraggiunte** anche in periodo estivo **dovrebbero aver portato il Governo a non attenersi troppo scrupolosamente allo spirito letterale dell'incredibile richiesta della Commissione parlamentare**, prevedendo invece che le regole tecniche rimangano in vigore e siano pienamente applicabili fino all'arrivo del nuovo DPCM (da emanarsi entro quattro mesi dall'entrata in vigore del nuovo CAD). Verrebbe meno, così, solo l'obbligatorietà per le PA di adeguarsi entro e non oltre la scadenza (ormai abbondantemente superata) del 12 agosto. Usiamo il condizionale perché, nonostante il comunicato stampa governativo del 10 agosto, nel quale si annunciava l'approvazione della riforma del Codice dell'amministrazione digitale e, quindi, l'avvenuta sospensione della fatidica scadenza del "digital first", del testo di legge ancora oggi non c'è traccia in Gazzetta Ufficiale! Crediamo che qualsiasi ulteriore commento sia superfluo.

Purtroppo situazioni simili le stiamo vivendo con il FOIA (Freedom of Information Act), riguardo al quale il disordine tra distinti diritti di accesso a cavallo tra diverse norme (tutte in vigore e in contraddizione tra loro) sta producendo i primi, inevitabili dubbi giurisprudenziali. Si fa riferimento alla recentissima sentenza del Consiglio di Stato sez. IV, del 14 luglio 2016, n. 3631, la quale contiene un netto rifiuto a una richiesta di accesso ex L. 241 formulata da un giornalista (che tra i primi aveva applaudito a questa "rivoluzione" normativa verso la trasparenza), dando l'occasione per affrontare criticamente la nuova confusionaria normativa contenuta in questo "foia" tutto italiano.

Stessa sorte sembra avere il processo telematico, che si va contorcendo nei meandri delle pec (nell'assenza – o, forse, sarebbe più corretto dire mancato rispetto - di rigide regole per la loro corretta fascicolazione e conservazione), e SPID (fermo a meno di 100.000 identità rilasciate in un deserto di PA davvero digitalizzate e con servizi attivabili on line).

Ma questi mutamenti improvvisi di rotta non devono scoraggiarci troppo: il cambiamento digitale c'è - sebbene proceda a un ritmo irregolare, fatto di strattoni, pause e qualche giro a vuoto – **ed è un processo inesorabile, al quale possiamo contribuire attivamente.**

Noi, nel nostro piccolo, intendiamo continuare a farlo diffondendo informazione, incentivando l'approfondimento e animando il dibattito in materia di digitalizzazione documentale e privacy: **a questo scopo abbiamo dato vita alla nuova rivista KnowIT.**

Questo primo numero "pilota" è un po' un'eccezione, essendo dedicato interamente alla pubblicazione degli atti del convegno dell'associazione AIFAG "FEA, biometria, privacy e compliance: il nuovo scenario europeo", tenutosi lo scorso 24 giugno a Lecce in cui massimi esperti del settore e rappresentati del mercato si sono confrontati apertamente su questi temi in relazione al regolamento

eIDAS e al nuovo regolamento europeo sulla privacy.

Più in generale, **KnowIT sarà una rivista digitale trimestrale gratuita, dal taglio operativo, dai contenuti il più possibile chiari, fruibili anche per i non esperti, a firma di autorevoli esperti nazionali, fornendo un valido apporto formativo, quindi, ai professionisti della digitalizzazione e della privacy**. I lettori a cui ci rivolgiamo sono infatti coloro che, per scelta o per forza, si trovano a dover gestire il delicato passaggio organizzativo dall'analogico al digitale e a "maneggiare" documenti informatici e dati personali. A nostro parere la vera chiave dell'innovazione sono proprio le loro competenze.

Mentre le norme si avvicendano e i progetti governativi si sovrappongono, a volte arenandosi, l'innovazione digitale può essere portata avanti in concreto solo grazie alla preparazione degli operatori. È estremamente importante, perciò, che chi si occupa di flussi di dati e documenti digitali nelle organizzazioni pubbliche e private acquisisca uno specifico know how e sia un vero "professionista dell'innovazione digitale", un manager del cambiamento sempre correttamente aggiornato sulle novità normative come sugli aspetti tecnici. KnowIT vuole essere, quindi, per i professionisti della digitalizzazione documentale e della privacy un ausilio formativo e uno strumento di approfondimento, magari contribuendo a fare chiarezza su qualcuna delle tante incertezze con cui i protagonisti di un'operazione pioneristica (e tale deve essere considerata la gestione di questo delicato momento di passaggio dalla carta al bit) si trovano a dover fare i conti.

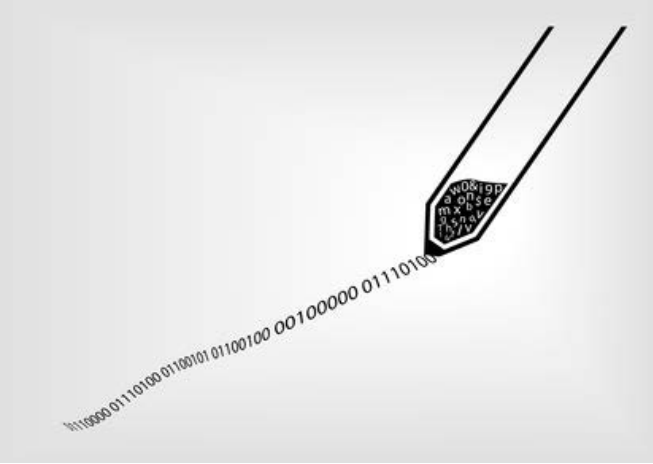
Formazione e buone pratiche contro incertezza e improvvisazione: solo così riusciremo a sfruttare appieno le sconfinate possibilità che il digitale ci offre, scansandone le possibili insidie.

Qual è la prospettiva europea dopo l'entrata in applicazione del Regolamento eIDAS?

Dott.ssa Elena Alampi - *DG CONNECT, European Commission*

Dall'1 luglio scorso eIDAS è diventata realtà, senza rimpianti per la Direttiva sulla firma che, a causa dei diversi adattamenti nelle legislazioni nazionali, ha portato alla formazione di un panorama europeo fortemente frammentato. **Oggi abbiamo un regolamento, eIDAS, direttamente applicabile a tutti i paesi UE, che garantisce sicurezza, certezza giuridica, affidabilità nelle transazioni elettroniche, tra imprese, cittadini e pubbliche amministrazioni**: un contributo importante per la realizzazione del Mercato Unico Digitale.

Non solo più firma, ma servizi fiduciari, con una certezza giuridica ma con valore probatorio differente. Firme, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati di autenticazione di siti web che possono essere usati ovunque nell'UE con un effetto giuridico equivalente ai corrispondenti cartacei, con un marchio di fiducia UE che permette di distinguere i servizi qualificati, che possiedono un valore giuridico più elevato, dai servizi fiduciari non-qualificati. Un marchio di fiducia che migliora certamente la trasparenza del mercato Europeo ma anche e soprattutto la fiducia degli utenti nelle transazioni elettroniche.



Un altro elemento di trasparenza è rappresentato dagli elenchi di fiducia pubblicati dai paesi UE che contengono le informazioni relative ai prestatori di servizi fiduciari qualificati, elenchi che già esistevano sotto la direttiva servizi ma che ora possiedono un effetto costitutivo, in quanto i prestatori sono considerati qualificati solo se figurano nell'elenco di fiducia.

Transazioni elettroniche più sicure, trasparenti, affidabili e facili d'uso, tutti ingredienti necessari alla realizzazione di un mercato unico digitale. Tutto ciò grazie a un quadro normativo olistico che trascende i confini nazionali e apre la strada a nuove opportunità per le imprese, le pubbliche amministrazioni e i cittadini, rendendo le interazioni digitali il nuovo modo naturale di comunicazione e stimolando di fatto l'innovazione e la trasformazione digitale.

Grazie, infatti, al passaggio a servizi e processi totalmente digitalizzati che permettono di ottenere delle economie di scala, **le imprese possono esplorare nuovi modelli di business, attirare un maggior numero di clienti ed espandere le quote di mercato al di là dei confini nazionali, realizzando un mercato unico digitale.**

È il caso di numerosi settori, dal settore finanziario al commercio elettronico, i trasporti, la sanità e la lista non è esaustiva come è stato recentemente evidenziato nel Piano d'azione eGovernment nel contesto della strategia per il Mercato Unico digitale lanciata un anno fa, in cui sono state identificate azioni volte ad accelerare l'uso transfrontaliero e intersettoriale dell'identificazione elettronica (eID), compresa l'identificazione mobile, e dei servizi fiduciari nei settori digitalizzati e nel settore pubblico.

Le opportunità sono evidenti ma occorre uno sforzo collettivo nei diversi settori per poterle cogliere. **È in quest'ottica che il Vice Presidente della Commissione Europea Andrus Ansip ha lanciato**, in occasione dell'evento il 30 giugno scorso, **l'Osservatorio eIDAS**, per offrire la possibilità alle parti interessate di discutere, confrontarsi, scambiare idee e buone pratiche sull'uso di servizi fiduciari e identificazione elettronica.

Perché è vero che dall'1 luglio eIDAS è applicato in relazione alle disposizioni sui servizi fiduciari, ma già da settembre 2015 i paesi UE possono notificare e riconoscere i mezzi di identificazione nazionali che cittadini e imprese potrebbero utilizzare per accedere agevolmente e in piena sicurezza a servizi pubblici online ovunque nell'UE. Oltre i servizi fiduciari, eIDAS regolamenta infatti anche il riconoscimento transfrontaliero di credenziali di identificazione e autenticazione elettroniche in uso nei paesi UE, e nel settembre 2018 gli Stati Membri avranno l'obbligo di riconoscere i sistemi che saranno stati notificati alla Commissione Europea dai diversi paesi UE.

In tale contesto, è importante sottolineare che oltre al quadro normativo che fornisce certezza giuridica, **l'UE si è dotata delle infrastrutture tecnologiche necessarie** sviluppate nell'ambito del programma CEF (Connecting Europe Facility) **per promuovere l'interoperabilità** dell'eID e dei servizi fiduciari. Attualmente, tra l'altro, c'è la possibilità di partecipare a un bando di gara - con scadenza il 15 settembre p.v. - messo a punto per promuovere l'integrazione dei meccanismi di identificazione nel contesto del quadro d'interoperabilità sotto eIDAS. Tutti i settori che presentano un alto volume di transazioni transfrontaliere sono chiamati a partecipare per collegare i loro servizi alla rete di interoperabilità per le transazioni transfrontaliere.

È una grande opportunità, non solo per il finanziamento in gioco, ma anche per la possibilità che il bando offre

alle imprese che partecipano di testare i collegamenti transfrontalieri attraverso il “nodo” eID sviluppato sotto CEF.

Opportunità che si offrono al settore privato grazie a credenziali di identificazione e autenticazione elettroniche sicure, interoperabili e riconosciute in tutta l’UE.

Da ultimo, diverse sono le iniziative portate avanti a livello europeo per promuovere ulteriormente queste opportunità e accelerare la diffusione dei mezzi di identificazione elettronica e dei servizi fiduciari. Nel contesto della strategia per il Mercato Unico digitale non è da dimenticare la promessa della Commissione nel Piano d’azione eGovernment di instaurare il principio di “digitale per definizione” nelle sue interazioni online con le parti interessate esterne, ricorrendo ai servizi eIDAS. O ancora, nella Comunicazione sulla standardizzazione delle TIC figurano iniziative volte a sostegno dell’interoperabilità globale e dell’autenticazione affidabile senza discontinuità tra dispositivi, oggetti, persone fisiche e giuridiche sulla base di modelli in linea con eIDAS. Infine, la promozione di azioni di interoperabilità delle identificazioni elettroniche (eID) nella Comunicazione sulle piattaforme online per incoraggiare le piattaforme online ad accettare altri mezzi di identificazione elettronica, in particolare quelli notificati sotto eIDAS.

eIDAS fornisce gli elementi chiave per garantire sicurezza, certezza legale, fiducia e convenienza nelle transazioni e servizi digitali a livello transettoriale e transfrontaliero. Molto resta da fare, e la strada davanti a noi non sarà senza ostacoli, ma le opportunità ci sono e bisogna saperle cogliere. Le opportunità, come le sfide, sono collettive e occorre percorrere la strada insieme per beneficiare di un Mercato Unico Digitale. E l’osservatorio eIDAS rappresenta un’ottima base per iniziare questo percorso insieme.

Gli attuali strumenti della digitalizzazione nel contesto del Regolamento eIDAS

Dott. Stefano Arbia - *Responsabile del Servizio Accreditamento, Certificazione e Vigilanza di AgID*

Il Regolamento n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 (eIDAS) è chiaramente orientato a rafforzare il concetto di cittadinanza europea, agevolando la fruibilità dei servizi online di tutte le pubbliche amministrazioni dell'Unione, ma anche il commercio elettronico.

Il Regolamento, che si applica a decorrere dal 1° luglio 2016, individua due categorie di servizi: i *servizi fiduciari* e i *servizi di identificazione elettronica*.

Fra i *servizi fiduciari* abbiamo la firma elettronica qualificata, la validazione temporale, il sigillo elettronico, i certificati di autenticazione per siti web, la posta elettronica certificata, e i servizi a loro afferenti.

Questi costituiscono una parte degli strumenti della digitalizzazione presenti nel nostro paese il cui fondamento è ricercabile nel Codice dell'Amministrazione digitale – CAD (D.lgs. 7 marzo 2005, n.82).

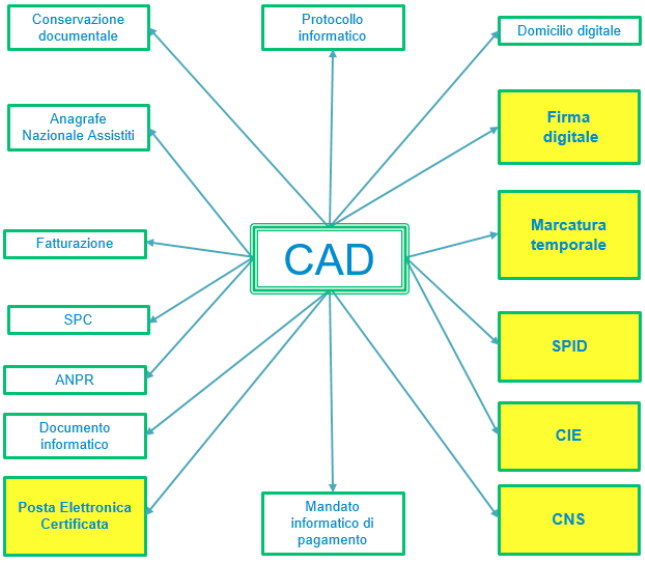


Figura 1- Strumenti per la digitalizzazione, evidenziati quelli previsti nel regolamento eIDAS

I servizi fiduciari possono assumere la denominazione e il valore di ***servizi fiduciari qualificati*** se soddisfano i requisiti del Regolamento e se l'autorità preposta nello Stato in cui sono stabiliti i prestatori di tali servizi - in Italia l'Agenzia per l'Italia Digitale (AgID) - ha riconosciuto tale *status* impegnandosi a effettuare la prevista vigilanza sugli stessi.

Fermo restando l'obbligo di vigilanza, fanno eccezione i *servizi fiduciari afferenti alla firma elettronica qualificata*, che sono immediatamente riconosciuti nell'Unione europea, quindi quelle che in Italia siamo soliti chiamare *firme digitali* o *firme elettroniche qualificate* continuano a essere utilizzabili e sono riconosciute nell'Unione europea.

Ma cosa possiamo aspettarci per gli altri servizi fiduciari utilizzati da anni nel nostro Paese?

Per poter ottenere lo *status* di *servizi qualificati* i servizi, su richiesta dei soggetti che li erogano, dovranno essere oggetto di valutazione da parte di AgID per poter essere riconosciuti e usati anche al di fuori del territorio nazionale.

Fino a tale riconoscimento, stante la normativa vigente al mese di luglio 2016, tali servizi continueranno a essere usabili e continueranno a produrre gli effetti previsti dalla legge nazionale.

Fra questi, un esempio è il servizio di **Validazione Temporale** che, si ricorda, consente di associare a un documento elettronico (di qualunque fattispecie, sottoscritto o meno) un riferimento temporale opponibile a terzi (la marca temporale). In pratica, la Validazione permette di dimostrare l'esistenza di un documento a una data e a un'ora certe.

All'inizio del mese di luglio 2016 già sono quattro i certificatori (prestatori di servizi fiduciari qualificati, nella terminologia del Regolamento) che hanno ottenuto tale riconoscimento e che sono quindi in grado di fornire il servizio di validazione temporale riconosciuto su tutto il territorio dell'Unione.

La **Posta Elettronica Certificata** (PEC) è da anni in uso nel nostro Paese, con oltre otto milioni di utilizzatori che producono circa duecento milioni di messaggi l'anno: per poter ottenere il riconoscimento di *servizio qualificato* ha bisogno di alcuni correttivi.

In particolare, è necessario che le caselle di PEC siano rilasciate dai gestori previo accertamento dell'identità del richiedente. Anche in questo caso, stanti le norme, continuerà a essere usabile nel territorio nazionale. Ciononostante, va notato che l'articolo 43.1 del Regolamento prevede che la trasmissione di dati con un sistema quale la PEC debba essere ammissibile come prova nei procedimenti giudiziali. Resta ancora da realizzare una soluzione che consenta l'immediato mutuo riconoscimento nell'ambito dell'Unione: infatti, contrariamente alla firma elettronica qualificata, non vi sono Atti esecutivi che ne regolino le caratteristiche tecniche.

Il Regolamento introduce due servizi, attualmente non normati nel nostro Paese: i *sistemi di autenticazione dei siti web* e il *sigillo elettronico*.

I primi hanno l'obiettivo di fornire una garanzia circa la reale paternità di un sito web ove siano disponibili servizi di diversa natura. Evidente è il vantaggio per il commercio elettronico: gli acquirenti possono avere una garanzia circa la reale identità del soggetto che espone il servizio.

Il sigillo elettronico tecnicamente è assimilabile a una firma elettronica qualificata afferibile a una persona giuridica: fornisce garanzie in merito all'origine (denominazione della persona giuridica) e all'integrità dei dati cui il sigillo è stato apposto. Il sigillo elettronico potrebbe costituire uno strumento per fornire delle garanzie in merito

all'impegno assunto da una persona giuridica. Peraltro, il sigillo elettronico non trova chiaro riscontro nel nostro ordinamento, attualmente sembrerebbe essere assimilabile a un timbro, limitando però le intenzioni del legislatore europeo. Sarebbe quindi auspicabile un'attività legislativa che ne indichi gli effetti giuridici e il reale ambito di applicazione in ottica comunitaria.

Ottenuto il riconoscimento di *servizio fiduciario qualificato*, il prestatore del servizio potrà utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati prestati.

Figura 2- Il marchio di fiducia UE

I ***servizi di identificazione elettronica*** sono destinati all'accesso ai servizi in rete. Fra questi, nel nostro Paese, abbiamo lo SPID, la Carta d'Identità Elettronica - CIE e la Carta Nazionale dei Servizi - CNS. Il Regolamento eIDAS non impone alcun vincolo agli Stati membri per la realizzazione di tali sistemi a livello nazionale, che restano "*liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica*" (considerando 13 del Regolamento).

Il Regolamento prevede, tuttavia, la possibilità di ottenere il mutuo riconoscimento di tali sistemi di identificazione elettronica in modo che siano usabili per accedere ai servizi di tutte le pubbliche amministrazioni dell'Unione europea.

A tale scopo, gli Stati membri interessati dovranno intraprendere una apposita procedura di notifica. La notifica è una interessante opportunità che sarà certamente colta anche dal nostro Paese. L'Agenzia per l'Italia Digitale provvederà nei tempi e modi opportuni.

Per notificare uno schema di identificazione elettronica è necessario che lo Stato membro notificante garantisca la funzionalità dello stesso in favore degli altri Stati membri.

A tale scopo, sono previste due possibilità: un'**interoperabilità architetturale o funzionale**.

Alcuni sistemi godono nativamente dell'interoperabilità architetturale, come la CIE e la CNS. Queste, infatti, utilizzano sistemi di autenticazione già in uso nei browser normalmente utilizzati.

Altri schemi, come lo SPID, richiedono la realizzazione dell'interoperabilità funzionale. A tale scopo, quando si scrive questo articolo, è già in fase di realizzazione il cosiddetto *nodo eIDAS*: si tratta di un servizio che fa da filtro (*middleware*) fra il richiedente (ad esempio la pubblica amministrazione di uno Stato membro) e il sistema nazionale. Quando un cittadino italiano richiederà di autenticarsi a un servizio di una pubblica amministrazione di un altro Stato membro, ad esempio utilizzando la propria identità digitale SPID, questa si rivolgerà al proprio nodo nazionale (*nodo eIDAS*) che, attraverso il *nodo eIDAS* italiano, sarà in grado di provvedere all'autenticazione (verifica dell'identità digitale) del cittadino, fornendo all'amministrazione richiedente le informazioni necessarie a identificarlo (nome, cognome, ecc.).

Visto il combinato disposto di alcuni articoli del Regolamento, il mutuo riconoscimento sarà obbligatorio per le pubbliche amministrazioni non prima del gennaio 2018 (ovvero non prima di diciotto mesi dall'avvio della procedura).

Premesso che il Regolamento individua tre livelli crescenti di credenziali per l'autenticazione (livelli di sicurezza ripresi dal legislatore nazionale nella realizzazione dello SPID), l'obbligo per le pubbliche amministrazioni riguarda l'accesso a tutti i servizi che esporranno in rete e che richiedono credenziali di livello 2 o 3.

Per evitare sorprese, è bene ricordare che il CAD dispone l'obbligo per le pubbliche amministrazioni nazionali di consentire l'accesso ai propri servizi in rete esclusivamente per mezzo delle credenziali SPID, oltre che CIE e CNS, a decorrere dal 18 dicembre 2017.

Come si è visto, **l'applicazione del Regolamento è obbligatoria per le pubbliche amministrazioni, mentre è facoltativa per i privati, almeno ad oggi**. Infatti, il Parlamento Europeo, già in prima stesura, aveva dichiarato l'intenzione di includere nell'ambito di applicazione anche i privati, intenzione non accolta da gran parte degli Stati membri. Durante i lavori presso il Consiglio europeo si è quindi stabilito di valutare in seguito tale estensione dell'ambito di applicazione, attraverso la procedura di riesame dell'applicazione del Regolamento, da svolgersi entro il 1° luglio 2020. Il riesame è previsto nell'articolo 49 che recita: "*La Commissione valuta in particolare se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, compresi l'articolo 6, l'articolo 7, lettera f), e gli articoli 34, 43, 44 e 45, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici*".

Regolamento eIDAS: le opportunità offerte dai sigilli elettronici e le altre novità per il nostro ordinamento

Avv. Sarah Ungaro - *D&L Department - Studio Legale Lisi, Vice Presidente ANORC Professioni*

Dal 1° luglio 2016 sarà direttamente applicabile il Regolamento UE 910/2014, c.d. eIDAS, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Si tratta di un regolamento self-executing, quindi direttamente applicabile negli ordinamenti nazionali. Tuttavia, com'è noto, per allineare le nostre norme a quelle di derivazione UE si discutono ormai da diversi mesi le modifiche al nostro Codice dell'Amministrazione digitale (D.Lgs. 82/2005).

Nello specifico, il Regolamento stabilisce le condizioni in base alle quali **gli Stati membri riconoscono reciprocamente i mezzi di identificazione elettronica delle persone fisiche e giuridiche notificati alla Commissione** da ciascuno Stato membro e statuisce le norme comuni relative ai c.d. **servizi fiduciari** ("trust services")[1], ossia inerenti alla:

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

b) creazione, verifica e convalida di certificati di autenticazione di siti web;

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

Proprio in tema di conservazione, è interessante rilevare che **i servizi di conservazione dei documenti informatici attualmente disponibili nel mercato digitale italiano potrebbero non essere immediatamente riconducibili nel novero dei servizi fiduciari elencati** al n. 16 dell'art. 3 del Regolamento eIDAS, in cui sarebbero ricompresi esclusivamente i servizi relativi alla *"conservazione di firme, sigilli o certificati elettronici relativi a tali servizi*", e dunque non anche i servizi di conservazione di qualsiasi documento informatico. Tuttavia, al considerando n. 25 del Regolamento si precisa che *"è opportuno che gli Stati membri mantengano la libertà di definire altri tipi di servizi fiduciari oltre a quelli inseriti nell'elenco ristretto di servizi fiduciari di cui al presente regolamento, ai fini del loro riconoscimento a livello nazionale quale servizi fiduciari qualificati"*. Ciò significa che **non è da escludersi che anche i servizi di conservazione attualmente forniti dagli operatori del mercato italiano possano essere riconosciuti a livello nazionale come servizi fiduciari qualificati**, qualora soddisfino i requisiti stabiliti dalle Regole tecniche del DPCM 3 dicembre 2013 ed eventuali ulteriori requisiti stabiliti da AgID.

Ulteriore elemento di particolare interesse nelle norme del Regolamento eIDAS risulta essere il **valore giuridico attribuito alle firme elettroniche qualificate**, **soprattutto in ottica comparativa con quanto disciplinato dal nostro CAD**: in effetti, in base all'art. 25 di eIDAS, a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per le firme elettroniche qualificate; in particolare, il comma 2 dello stesso articolo 25 stabilisce che "***una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa***". Ciò significa che – in assenza del disposto dell'art. 21 del CAD - l'apposizione di una firma elettronica qualificata avrebbe l'efficacia giuridica prevista dall'art. 2702 c.c. e quindi sarebbe disconoscibile ai sensi dell'art. 214 c.p.c.: **nel nostro ordinamento, invece, il secondo comma dell'art. 21 del CAD attribuisce alle sole firme elettroniche qualificate e digitali una presunzione legale di riconducibilità del documento al firmatario**[2]. Ciò significa che, rispetto al diverso e più generico valore giuridico e probatorio previsto dal regolamento eIDAS, alla luce del nostro CAD non è sufficiente procedere al disconoscimento di una firma elettronica qualificata per contestarne l'efficacia probatoria, ma si configura un'inversione dell'onere della prova tale per cui è il titolare della firma elettronica qualificata o digitale a dover produrre la concreta prova contraria, idonea a dimostrare, con ragionevole certezza, che egli non sia stato l'autore della sottoscrizione effettuata con il dispositivo di firma di cui era titolare. In tal senso, è lo stesso considerando n. 49 del regolamento eIDAS a precisare che **spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche**, fatta salva l'equivalenza dell'effetto giuridico di una firma elettronica qualificata a quello di una firma autografa stabilita dallo stesso Regolamento.

In modo speculare alle firme elettroniche, **il regolamento eIDAS disciplina i sigilli elettronici**, finora sconosciuti nel nostro ordinamento, che hanno la funzione di **fungere da prova della provenienza o dell'autenticità di un documento elettronico** - come di qualsiasi oggetto informatico (quali, ad esempio, codici software o registrazioni di log o video-audio) – **da parte di una determinata persona giuridica** (creatore del sigillo), dando la certezza dell'origine e dell'integrità dello stesso. In particolare, l'art. 35, comma 2, del Regolamento stabilisce **una presunzione legale di integrità e di correttezza dell'origine del documento a cui è associato un sigillo elettronico qualificato: tale effetto giuridico è in ogni caso**

implicitamente attribuito anche alle firme elettroniche qualificate dal Regolamento eIDAS che, al considerando n. 58, prevede che qualora una transazione richieda un sigillo elettronico qualificato di una persona giuridica, è opportuno che sia accettabile anche la firma elettronica qualificata del rappresentante autorizzato della persona giuridica.

A ben vedere, infatti, è possibile apprezzare **la diversa funzione di una firma elettronica** (che il Regolamento eIDAS ricollega in ogni caso ai dati del "firmatario" persona fisica) **e di un sigillo elettronico** (che lo stesso Regolamento ricollega ai dati del "creatore del sigillo" persona giuridica) riprendendo le funzioni della sottoscrizione individuate da Carnelutti, che attribuiva all'apposizione della firma una funzione c.d. indicativa (necessaria a identificare il soggetto al quale la firma – o lo strumento di firma elettronica - appartiene), una funzione c.d. probatoria (per provare la provenienza di un documento), ma anche una funzione c.d. dichiarativa (per provare il consenso, la volontà, l'approvazione o la ratifica del contenuto del documento). Proprio tale ultima funzione, attribuita da Carnelutti all'apposizione di una firma, risulta essere invece assente **nell'apposizione di un sigillo elettronico, a cui possono essere ricollegati solo gli effetti giuridici di integrità**[3] **e autenticità del documento, comunque riconosciuti anche all'apposizione di una firma elettronica qualificata**[4].

Ma quali potranno essere, dunque, **i possibili utilizzi di un sigillo elettronico** (eventualmente prevedendo anche delle piccole modifiche alle norme attualmente vigenti nel nostro ordinamento)? Innanzitutto, i sigilli potranno essere utilizzati per le fatture elettroniche fra soggetti privati (per cui l'utilizzo di un sigillo avanzato è già previsto nella bozza di specifiche tecniche predisposte dall'Agenzia delle Entrate) e per le fatture elettroniche verso la PA (modificando l'Allegato B al DM 55/2013); per la pubblicazione degli atti nell'Albo pretorio on line da parte del Responsabile della pubblicazione; per il Pacchetto di Archiviazione del sistema di conservazione (modificando il DPCM 3 dicembre 2013); per le copie per immagine di documenti originariamente analogici e le copie informatiche di documenti informatici; per le estrazioni statiche di registrazioni informatiche, come i file di log, previste dall'art. 3 del DPCM 13 novembre 2014; per gli atti e i documenti depositati nel processo civile telematico, in sostituzione del timbro della Cancelleria che veniva apposto in caso di deposito cartaceo e, in generale, **in tutti i casi in cui non sia necessario «sottoscrivere» un documento, ma sia sufficiente garantirne l'origine, l'autenticità e l'integrità**.

Note

1. Definiti come servizi elettronici forniti normalmente dietro remunerazione.
2. Art. 21, comma 2, del CAD: "L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria".
3. In particolare, il Regolamento eIDAS prevede nell'art. 35, 2° comma che "un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico è associato". Analoga presunzione, in verità, non è prevista espressamente nel Regolamento anche per le firme elettroniche qualificate, ma appare corretto comunque che sia ritenuta implicita, anche alla luce del menzionato considerando n. 58.
4. Da qui la considerazione che ove sia apposta una firma elettronica qualificata o digitale appare inutile l'apposizione anche di un sigillo elettronico, ma non viceversa.

Un particolare caso di compliance aziendale: la Pubblica Amministrazione Locale. Quali le novità?

Avv. Giovanni Maglio - *Commissione informatica Ordine Avvocati di Lecce*

Nel settore della Pubblica Amministrazione, specie quella locale, le questioni sottese al trattamento dei dati personali sono sempre state connotate da un diffuso atteggiamento di superficiale ritrosia, in quanto la c.d. privacy è, quasi dappertutto, vissuta come un inutile orpello che va a ingolfare le già farraginose ed elefantiache macchine amministrative.
Macchine amministrative che spesso vengono guidate in maniera non lineare, specie per ciò che riguarda la loro modernizzazione, attraverso l'invisa innovazione tecnologica e l**a faticosa applicazione delle ICT e del digitale a quelli che, a ben guardare, sono dei veri e propri processi produttivi (di servizi pubblici)**, in quanto tali, ottimizzabili.
Eppure, ormai la strada per le PA è inequivocabilmente segnata nella direzione del digitale e non è possibile tornare indietro. Ne consegue, quindi, che l'imperativo è adeguarsi o… pagare!
E sì, perché **il mancato adeguamento alle normative sull'innovazione e sul trattamento dei dati personali** (mai come ora strettamente interconnesse) **comporta un notevole rischio di sanzioni** (quanto meno civili e disciplinari, ma senza trascurare le penali) **a carico delle amministrazioni inadempienti** e per esse ai loro dirigenti, in primis.
In tale contesto, la normativa sul trattamento dei dati personali ricopre un ruolo di primaria rilevanza, chiamando le PA a operare in piena conformità alle disposizioni di riferimento.

Normative che nel prossimo biennio sono destinate a essere profondamente modificate, in considerazione della definitiva applicazione del Regolamento UE n. 2016/679.
Tale strumento europeo incide profondamente sul quadro normativo che, da quasi vent'anni, siamo abituati a conoscere, introducendo modifiche che forniscono l'occasione di migliorare il funzionamento delle PA, anche attraverso il rafforzamento della tutela dei diritti; ne consegue che quest'occasione non può essere sprecata, ma, anzi, deve essere colta in ogni suo aspetto, affinché il passaggio della pubblica amministrazione dalla dimensione analogica a quella digitale sia effettivo e concreto.
Il countdown è iniziato: dal 25 maggio 2018, il nuovo regolamento privacy avrà piena applicazione in tutta Europa. Questa è una prima grande novità, insita nella sua natura di Regolamento, automaticamente applicabile, senza necessità di recepimento interno da parte degli stati membri, a differenza di una semplice direttiva.
Per quanto riguarda gli adeguamenti previsti, **il restyling delle informative ai sensi dell'art. 12 del Regolamento rappresenta un primo ambito di intervento**; vengono, infatti, banditi quei lunghi testi spesso infarciti di noiosissimi e incomprensibili riferimenti normativi che hanno sinora privilegiato la forma sulla sostanza.
Le nuove informative dovranno essere adottate attraverso misure appropriate perché all'interessato vengano fornite tutte le informazioni di cui agli articoli 13 e 14 (tra cui identità e dati di contatto del titolare, finalità del trattamento, base giuridica, periodo di conservazione, esistenza dei diritti di cui agli artt. 15-21); la forma dovrà essere concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
In tale ambito, vi è anche un'apprezzabile iniziativa europea che prevede l'introduzione di icone e simboli di facile riconoscibilità e immediata intuitività, ma soprattutto di comune applicazione.
Che segni una svolta per il legal design? Staremo a vedere!
Il **sito web**, adeguatamente realizzato, si pone come una delle migliori interfacce per assolvere a tale compito.
Capitolo di grandissima rilevanza, poi, è quello che riguarda **l'adeguamento delle misure di sicurezza**, che dovrà essere effettuato sulla base dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.
Il Regolamento elimina la distinzione tra minime e idonee, indicando alcune di queste misure di sicurezza, tra le quali la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Per chiudere il cerchio, ed evitare il lassismo che spesso dilaga nell'effettuare il monitoraggio continuo, viene fatta rientrare tra le misure di sicurezza anche una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Per cui ben vengano le best practice di ogni P. A. nell'attuare le misure di protezione dati: misure tecniche, informatiche, organizzative, logistiche e procedurali.
L'art. 30 introduce **la novità del Registro delle attività di trattamento**, stabilendone la sua istituzione e indicandone il contenuto minimo (nome e dati di contatto del titolare

del trattamento, finalità del trattamento, descrizione delle categorie di interessati e delle categorie di dati personali, categorie di destinatari a cui i dati personali sono stati o saranno comunicati).
In una PA ormai votata al digitale, tale registro dovrà necessariamente essere tenuto in formato elettronico, coerentemente con le normative del CAD e del Regolamento eIDAS.
Due aspetti intimamente collegati tra di loro, poi, sono **la redazione della PIA (Privacy Impact Assesment) e l'applicazione dei principi privacy by default e by design**.
Questi istituti non sono del tutto nuovi nel panorama della privacy, ma adesso trovano un puntuale riferimento normativo (artt. 35 e 25) che li estende e fa assurgere a momenti fondamentali per effettuare correttamente un trattamento di dati personali.
Si pensi, ad esempio, alla necessità di adeguare i procedimenti amministrativi alle logiche digitali, effettuando un'attività di reingegnerizzazione degli stessi, per semplificarli e digitalizzarli. Ebbene, tale operazione non solo dovrà necessariamente essere preceduta da una PIA - al fine di evitare pregiudizi in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, derivante dall'uso di nuove tecnologie - ma dovrà anche essere progettata, dall'inizio e per impostazione predefinita, affrontando e risolvendo tutte le problematiche privacy.
Un'altra peculiarità per le PA potrebbe essere rappresentata dall'art. 89, che prevede garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, e che potrebbe avere ricadute per quanto riguarda la, ormai imprescindibile, attività di conservazione digitale di cui al DPCM 03.12.2013. Tali garanzie devono assicurare che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati.
Ulteriore specifico obbligo imposto alle PA dall'art. 37 è la nomina del DPO (Data Protection Officer), una figura già esistente a livello europeo e adesso estesa anche ad altri titolari di trattamento, tra cui, appunto le PA, con compiti di informare e fornire consulenza al titolare del trattamento, sorvegliare l'osservanza delle normative relative alla protezione dei dati, fornire, se richiesto, un parere in merito alla PIA e sorvegliarne lo svolgimento, cooperando con l'autorità di controllo e fungendo da punto di contatto per la stessa.
Un imprescindibile parallelismo di tale figura va operato con quella che sembra sicuro verrà introdotta con la riforma del Codice dell'Amministrazione Digitale in corso di approvazione: il **Chief Digital Officer**. Si tratta di due figure che dovranno necessariamente operare nella massima intesa reciproca, condividendo strategie e obiettivi. Il Garante Privacy, con un suo apposito parere, si è addirittura espresso nel senso di far coincidere nella stessa persona tali ruoli; sommessamente, si ritiene che tale opinione non sia del tutto condivisibile, sia per le diversità dei ruoli sia per la cattiva abitudine delle PA di concentrare in capo a un solo soggetto troppi ruoli e responsabilità, che è più opportuno mantenere separati.
Altro **obbligo** esteso a tutti i titolari, comprese le PA, è quello **della notifica di violazione c.d. Data Breach** (artt. 33 e 34), attualmente limitato a poche e specifiche fattispecie.
Sul versante diritti degli interessati, la conferma rafforzata di molti diritti già esistenti, accanto alla introduzione di nuovi (previsti dagli artt. da 15 a 21), impone alle PA di essere pronte a rispondere alle richieste degli interessati, in maniera tempestiva e pertinente.
Ovviamente, l'utilizzo di database interoperabili, di logiche di cooperazione applicativa e lo scambio di dati tra pubbliche amministrazioni, in parte riducono tali diritti (specie quello alla portabilità) ma esigono, oltre alla sicurezza informatica, il rispetto delle garanzie di trasparenza verso i cittadini in merito agli obiettivi che si intendono perseguire e alle modalità per farlo.
Piccolo accenno merita anche il **trasferimento dei dati all'estero** - soprattutto per il respiro europeo del Regolamento che si abbina alla libera circolazione delle persone e dei loro dati personali – ma ancor di più **l'utilizzo di risorse in cloud computing**, le quali necessitano della adeguata conoscenza dei rischi insiti in tale tecnologia, proprio relativamente al trasferimento dei dati.
Infine, uno degli aspetti più peculiari e problematici, ma dalle potenzialità immense, è quello relativo alla **trasparenza**, spesso declinato in forma di ossimoro rispetto alla privacy, quando, invece, rappresenta una risposta importante a quel crescente afflato partecipativo e di sindacato diffuso sulla gestione della cosa pubblica.
La disciplina sulla trasparenza ha subìto una progressiva estensione, che ha portato a un'esigenza di razionalizzazione e ridefinizione degli obblighi di pubblicità, non del tutto colta dal recente decreto correttivo del D. L.vo 33/2013, così come sostenuto anche dal Garante Privacy nella sua audizione annuale al Senato.
Del resto, le PA dispongono di un patrimonio informativo dal valore immenso quanto sottovalutato e del quale dovrebbero tendere a sbloccare completamente il potenziale. Tuttavia le opportunità degli open data, del riutilizzo delle informazioni del settore pubblico e delle capacità di analisi dei Big data richiedono sia attenzione con riferimento alla sicurezza dei sistemi e delle infrastrutture utilizzate, sia la definizione di un ragionevole equilibrio tra valorizzazione del patrimonio informativo pubblico e garanzia di tutela dei diritti.
In conclusione, è bene continuare a studiare la nuova normativa per poterla adattare agli specifici casi concreti, nell'attesa che il Legislatore italiano e il Garante intervengano, ciascuno nel proprio ambito, a colmare gli spazi di discrezionalità che il Legislatore europeo ha lasciato.
E per fare ciò, i poco meno di due anni rimasti iniziano a sembrare pochi...

eIDAS: la buona occasione per cambiare il processo telematico!

Avv. Paolo Lessio - *Esponente del Direttivo del Circolo dei Giuristi Telematici*

L'entrata in vigore del regolamento eIDAS pone, evidentemente, la questione del se e del come tale regolamento impatterà sul nostro processo: già telematico quello civile e ancora da informatizzare tutti gli altri!
Una disamina puntuale impone però di prendere le mosse dall'attuale stato dell'arte del processo telematico così come oggi è disegnato dalla normativa tecnica e da quella più squisitamente processuale.
Il processo telematico funziona, peccato che al momento della sua obbligatorietà fosse già vecchio.
Innanzitutto è bene tenere presente che, come accennato più sopra, ad oggi l'unico rito processuale realmente informatizzato a livello nazionale e a regime è quello civile, nelle sue declinazioni del rito contenzioso (compreso quello del lavoro), di quello esecutivo e di quello fallimentare (limitatamente agli atti degli organi della procedura).
Sarebbe dovuto entrare già in vigore anche il processo amministrativo telematico ma, si sa, il nostro legislatore ama i colpi di scena e a pochi minuti dalla sua entrata in vigore è stato disposto un rinvio al 1° gennaio 2017. Il processo tributario, poi, è ancora una realtà locale e pochissime nuove, invece, arrivano dal fronte del processo penale. Si tenga poi conto del fatto che a essere informatizzati sono solo le cancellerie e i Giudici, mentre gli UNEP restano totalmente fuori dal sistema, arroccati alla carta come in una novella di Verga. Ciò che è certo in questa giustizia informatizzata a macchia di leopardo è che il legislatore, oltre a non fare mai scelte del tutto coraggiose nella direzione dell'informatizzazione reale sta, sostanzialmente, adottando soluzioni tecnologiche differenti per ogni tipo di processo - imponendo agli avvocati di diversificare non solo le loro competenze giuridiche ma anche quelle informatiche (a tutto vantaggio delle iniziative formative e a discapito della tranquillità dei difensori) - e moltiplicando, nei fatti, i rischi di invalidità processuali degli atti, a tutto svantaggio della giustizia sostanziale.
Ma non solo.
Sia chiaro che l'aria vagamente critica di questo articolo non deve trarre in inganno: il PCT funziona ed è stato un momento determinante (ed efficace) nella strada dell'innovazione della giustizia, ma ha ormai fatto il suo tempo e le attuali norme di rito funzionano con strumenti che, all'epoca del cloud e delle blockchain, risultano ormai superati e inidonei a tenere il passo con una evoluzione giuridico/culturale che, oggi più che mai, necessita di certezza e semplicità.
Oggi il PCT si basa ancora su un misto di carta (la notifica alle parti private preclude infatti in radice l'uso di un qualunque strumento telematico e il principio di unicità del titolo esecutivo non ha ancora trovato un approdo tecnologico o, forse meglio, l'abrogazione), firma digitale e PEC, che conducono una coesistenza obbligata all'ombra di un codice di rito che risale al 1942 e i cui principi non sono mai stati oggetto di una seria revisione tecnologicamente orientata ma solo di aggiustamenti disorganici capaci unicamente di trovare compromessi tecnologici tra il sistema tradizionale e la domanda di efficienza proveniente dagli uffici giudiziari.
Si consideri solo il meccanismo di deposito con il quale l'avvocato "introduce" un proprio atto nel fascicolo telematico: tale meccanismo impone ancora oggi **l'intervento manuale del cancelliere**. Tale intervento crea un divario temporale importante tra il momento del deposito di un atto e la sua visibilità e ha creato (e crea) diverse incertezze sulla validità di alcuni depositi, pur in presenza di un dato normativo inequivocabile.
E ancora si consideri, ad esempio, la già citata **estraneità degli UNEP a ogni procedura telematica** che, unitamente a una normativa davvero poco coraggiosa (anche se performante) in tema di notifiche a mezzo PEC, spesso impone all'avvocato di tornare alla carta per notificare; oppure anche **la scarsa chiarezza (o forse sarebbe più corretto dire la totale assenza) di principi in tema di conservazione documentale dei fascicoli giudiziari** su cui lo stesso Ministero mantiene un preoccupante silenzio.
Ma c'è di più.

La crisi che ha colpito l'intero sistema mondiale ha fatto sì che le aziende (non solo quelle specializzate in recupero crediti e NPL ma anche le c.d. piccole medie aziende e i gruppi di imprese) recuperassero un forte interesse all'accesso diretto al fascicolo (la banale attività di recupero crediti impatta, come noto, in maniera importante nel bilancio delle imprese che dunque vogliono essere regolarmente e puntualmente informate), che oggi impone all'azienda importanti investimenti in infrastrutture informatiche e formazione degli operatori.
Da ultimo, si tenga presente che l'attuale sistema non è in alcun modo progettato per interagire con documenti probatori originariamente informatici, lasciando dunque alla buona volontà del magistrato ogni approfondimento sul punto.
Così, descritto per sommi capi l'attuale sistema, conviene chiedersi quale direzione dovrebbe prendere il processo

telematico per essere maggiormente funzionale e quale apporto potrebbero dare i principi descritti nel regolamento eIDAS.
Si tenga presente che se il sistema odierno è caratterizzato dalla rigidità e dal formalismo (spesso inutile), il regolamento di cui si discute è invece un'opera fondamentalmente improntata alla definizione di principi e di contenuti in esatta contrapposizione con le problematiche accennate sopra e con l'intento evidente di rendere le nuove tecnologie una vera opportunità.
L'esperienza dell'attuale processo telematico ha evidenziato innanzitutto l'assoluta centralità del fascicolo, da intendersi come momento di condivisione degli atti e dei dati giuridici da parte di tutti i soggetti coinvolti nel procedimento.
Tutto il sistema, dunque, dovrebbe fondarsi su di un fascicolo informatico condiviso tra tutti gli attori del procedimento, che devono poter prendere visione dello stesso secondo quanto previsto dall'art. 6 comma I del regolamento eIDAS. Il regolamento europeo, così calato nell'operatività processuale, garantirebbe dunque:
- la riservatezza del dato: assicurata, dal punto di vista sistemico, da un livello di garanzia del regime di identificazione significativo o elevato (secondo le definizioni del comma 2c dell'art. 8 di eIDAS) a seconda del ruolo di chi accede e dell'importanza dell'attività cui tale soggetto deve dare corso;
- l'accessibilità totale (anche transfrontaliera) del fascicolo: se il fascicolo fosse gestito dalla PA, infatti, il regime di identificazione elettronica dovrebbe necessariamente essere soggetto alla procedura di notifica prevista dall'art. 7 del regolamento.

Un accesso così congegnato consentirebbe alla parte (anche ove si tratti di un'azienda) di prendere direttamente conoscenza dello stato e degli eventi del fascicolo: si pensi all'importanza di tale risvolto nei procedimenti di volontaria giurisdizione che, in taluni casi, possono essere direttamente introdotti dalla parte, nonché l'accessibilità del fascicolo, sulla base di standard condivisi, anche per tutti i professionisti ausiliari del Giudice (CTU, custodi, delegati alle operazioni di vendita ecc.) il cui accesso ad oggi risulta talvolta precluso.
Anche in tema di deposito, poi, **l'accesso diretto al fascicolo potrebbe essere ulteriormente implementato, a vantaggio della semplicità del deposito, con forme di sottoscrizione meno rigide di quelle attuali** (ad oggi l'unica tecnologia ammessa è quella della doppia chiave asimmetrica) e più user friendly (firma grafometrica?) da usare in relazione al livello di identificazione previsto per l'accesso.
Diventa quindi prospettabile un'operatività, oggi impossibile anche solo da immaginare, che vede il cliente privato (normalmente privo di strumenti tecnologici avanzati) firmare la procura all'avvocato direttamente in studio con firma grafometrica e l'utilizzo della stessa da parte dello stesso avvocato difensore.
eIDAS poi, laddove lascia, al 25° considerando delle premesse, la libertà di definizione (e di progettazione) dei servizi fiduciari prestati dai soggetti a ciò deputati, apre un intero mondo di possibilità, funzionali proprio a garantire le esigenze del processo.
Tanto per fare un esercizio di fantasia (e senza pretesa di correttezza o completezza di ciò che veramente si potrebbe fare con gli strumenti previsti in forza del regolamento eIDAS), si immagini la possibilità, sin dall'introduzione del procedimento, di gestire l'accessibilità dell'UNEP al fascicolo medesimo affinché estragga e provveda alla notifica di quegli atti che devono essere notificati cartaceamente. La conformità dei vari atti nelle varie forme potrebbe essere gestita tramite servizi tecnologici (glifo? sigilli elettronici della PA?) resi da prestatori di servizi fiduciari qualificati che garantiscano la continuità dei contenuti nelle varie forme dell'atto.
Oppure, ancora, si pensi a come l'accesso al fascicolo e il deposito degli atti possano essere confermati da documenti corredati automaticamente da sigilli elettronici (Sezione 5 del Regolamento) e validazioni temporali (Sezione 6 del Regolamento).
Inutile aggiungere poi che **un sistema così progettato potrebbe azzerare le distanze (garantendo a qualunque processo europeo che fosse informatico di diventare transfrontaliero)**, prevedere sistemi di verifica anche dei documenti probatori (la cui formazione da parte dei privati dovrebbe aumentare in virtù del medesimo regolamento) e interazioni tra diverse PA (si immagini la trascrizione automatica del pignoramento fatta all'atto dell'iscrizione a ruolo della procedura esecutiva immobiliare).
Per concludere: è evidente che eIDAS costituisce il primo vero pretesto, per il nostro legislatore, per prendere coscienza degli attuali limiti del sistema e progettare il processo del futuro in un'ottica di semplificazione ed efficienza a tutto vantaggio della certezza del diritto e dell'efficienza della giustizia.

Il nuovo Regolamento privacy e la sua adozione: elementi di novità e continuità

Avv. Graziano Garrisi - *D&L Department - Studio Legale Lisi, esponente del Direttivo ANORC*

Il 24 maggio 2016, dopo un periodo di gestazione durato quasi quattro anni, è stato pubblicato in Gazzetta Ufficiale dell'Unione Europea il Regolamento UE n. 679/2016 ovvero il "Regolamento generale sulla protezione dei dati". La portata di questa nuova regolamentazione comunitaria è dirompente perché, a circa 20 anni di distanza dalla prima forma di regolamentazione della privacy in Italia[1], si introduce un nuovo quadro giuridico di stampo europeistico in materia di protezione dei dati che, di fatto, traccia una nuova strada verso quella che potremmo definire una "Privacy 3.0".

Si tratta di un Regolamento c.d. "**self executing**", in quanto direttamente applicabile in ciascuno degli Stati membri dell'UE senza necessità di una legge nazionale di recepimento, il quale utilizza ai fini dell'applicazione (territoriale e materiale) delle sue disposizioni il criterio dello "stabilimento" (ovvero il luogo in cui è ubicata la sede principale delle attività del titolare o del responsabile del trattamento) affiancato dal criterio del "**targeting**" (che si sostanzia nell'offerta di prodotti o servizi destinati a soggetti presenti nel territorio UE); nello specifico si applica:

- all'offerta di beni o prestazione di servizi a interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento da parte dell'interessato[2];
- al monitoraggio del comportamento degli interessati nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il Regolamento effettua in diverse occasioni un **rinvio al legislatore nazionale** (che forse rischia, in taluni contesti, di vanificare le originarie intenzioni di garantire uniformità) per adattare alcune delle sue parti al diritto interno dei singoli Stati membri dell'UE, ciò **soprattutto con riguardo a specifiche tipologie di trattamento** (in particolare in ambito sanitario, ma anche rispetto ai trattamenti di dati genetici o biometrici, ai criteri di nomina di un DPO, alla possibilità di richiedere autorizzazioni da parte dell'Autorità di controllo per taluni trattamenti, alle norme che devono disciplinare istituzione e componenti delle Autorità di controllo, alla possibile previsione di sanzioni, anche penali, ulteriori rispetto a quelle contenute nel Regolamento etc.).

L'attuale quadro giuridico nazionale privacy, pertanto, sarà sostituito dal nuovo Regolamento, ma non completamente: **alcune delle Linee Guida, dei Provvedimenti e degli altri interventi emanati dal nostro Garante in tutti questi anni**, se compatibili e non in conflitto con la nuova regolamentazione, **rimarranno in vigore**.

Molto importante è il nuovo concetto di "**accountability**" (che nel Regolamento è stato tradotto con il termine "responsabilizzazione"): il titolare del trattamento, infatti, deve essere in grado di dimostrare di aver adottato un processo complessivo di misure giuridiche, organizzative, tecniche per la protezione dei dati personali (una sorta di "Modello" di organizzazione, gestione e controllo) e per la verifica che le misure adottate siano anche efficaci al fine di prevenire trattamenti illeciti sui dati o danni in capo agli interessati.

Dal punto di vista della regolamentazione dei ruoli e delle responsabilità in materia di trattamento dati, viene **ridisegnato l'organigramma privacy**, con l'introduzione di nuove figure soggettive e l'attribuzione/ripartizione di nuovi compiti e responsabilità.

Le (vecchie e nuove) figure soggettive previste, infatti, sono:

- Titolare del trattamento (data controller);
- Contitolare (joint controller);
- Responsabile del trattamento (data processor);
- Sub-responsabile (subprocessor);
- Responsabile della protezione dei dati o Data Protection Officer (DPO).

Soprattutto il rapporto tra Titolare e Responsabile (e di conseguenza tra Responsabile e sub-Responsabile) viene regolamentato in maniera specifica con **la previsione dei contenuti che devono essere inseriti nel relativo accordo contrattuale** (infatti, l'*esecuzione dei trattamenti su commissione è disciplinata da un* ***contratto o da altro atto giuridico*** *che vincoli il Responsabile del trattamento al Titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*) e ciò in maniera molto più dettagliata – forse limitando anche un po' quella autonomia e libertà contrattuale che dovrebbe sempre essere concessa alle parti - rispetto a quanto avveniva prima nel Codice Privacy italiano (d.lgs. 196/2003), che si limitava a richiedere l'analitica specificazione dei compiti

affidati al responsabile e delle istruzioni impartite dal titolare (art. 29, comma 4, del Codice citato).

Sarà importante procedere, quindi a una sistematica **revisione della contrattualistica e di tutti gli accordi** (attraverso nuovi privacy agreement o privacy level agreement, data transfert agreement, contratti di outsourcing, addendum contrattuali in materia di privacy etc.) che regolano la condivisione o lo scambio di dati personali tra l'azienda titolare del trattamento e tutti i soggetti sopra elencati.

Innovativa per il nostro ordinamento giuridico è, inoltre, la **nuova figura del Data Protection Officer (DPO)** o **Responsabile della Protezione dei dati** (da non confondere con il nostro Responsabile del trattamento ex art. 29 del D.Lgs. 196/2003), che è prevista come **obbligatoria per tutti gli enti pubblici e le pubbliche amministrazioni** e quando:

- le attività principali del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il **monitoraggio regolare e sistematico degli interessati** su larga scala[3];
- le attività principali del Titolare del trattamento o del Responsabile del trattamento consistano nel trattamento, su larga scala, di **categorie particolari di dati personali** idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché nel trattamento di dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati.

In particolare, **il DPO può essere individuato tra il personale dipendente in organico, oppure è possibile procedere a un affidamento di tale incarico all'esterno, in base a un contratto di servizi**, riferendo direttamente al vertice gerarchico del Titolare o del Responsabile del trattamento: assume una particolare rilevanza, pertanto, la corretta contrattualizzazione del servizio affidato (soprattutto in termini di garanzie per le attività che saranno svolte), in cui devono essere specificati e richiamati i compiti elencati all'art. 39 del nuovo Regolamento, sebbene si tratti sempre di un nucleo minimo di attività[4] che può essere affidato a un DPO (si legge nel preambolo di tale articolo, infatti, che "*il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti*"). Quello del DPO, in buona sostanza, può essere considerato un ruolo manageriale o di consulenza (di alto livello), controllo e vigilanza (assimilabile, ma non sovrapponibile, con l'Organismo di Vigilanza ai sensi del D.Lgs. 231/2001), che garantisce, assicura e contribuisce a elevare lo standard qualitativo della compliance aziendale in materia di privacy all'interno dell'organizzazione presso la quale svolge la propria attività, tanto da risultare anche un punto di riferimento per gli interessati e l'Autorità Garante[5].

Possiamo affermare, in conclusione, che sebbene i nuovi adempimenti siano tanti (e impongano, tra l'altro, un cambio di prospettiva nell'applicazione pratica dei nuovi principi), non bisogna essere allarmisti: **la normativa italiana, con il D.Lgs. 196/2003, partiva già da un buon livello di tutela della privacy** (molto elevato rispetto agli standard degli altri Sati europei), perché la Direttiva 95/46/CE (i cui principi sono stati semplicemente enfatizzati dal nuovo Regolamento europeo) era già recepita in maniera piuttosto stringente e molti provvedimenti - generali e speciali - della nostra Autorità Garante avevano inoltre contribuito a elevarne lo standard. Si tratta, quindi, di una soluzione di continuità e non tanto di una rivoluzione come molti dicono; è ovvio che ci sarà la necessità di gestire una fase di cambiamento, soprattutto perché si dovranno abbandonare gli inutili formalismi che la vecchia normativa imponeva, in favore di un approccio alla privacy basato più sull'analisi dei rischi e sulla preventiva adozione e implementazione di specifiche misure organizzative e di sicurezza, che forniscano garanzie e meccanismi di protezione più efficaci per i diritti e le libertà degli interessati.

Note

1. Ricordiamo che la prima norma in Italia è stata la 675 del 1996, seguita poi dal D.Lgs. 196/2003.
2. Nei Considerando si legge che "*Se la semplice accessibilità del sito web del titolare del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, e/o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare del trattamento di offrire beni o servizi a detti interessati nell'Unione*".
3. Concetti di "attività principali" e "larga scala" ancora poco chiari in quanto il Regolamento non fornisce una definizione chiara e precisa, ma si limita a fornire una spiegazione sommaria solo nei Considerando 91) e 97), in cui si precisa che si tratta di attività che "*mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti*" per il concetto di "larga scala" ovvero "*…le **attività principali** del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*".
4. Riassumendo, il DPO deve informare e fornire consulenza al Titolare o al Responsabile del trattamento (compresi i dipendenti che eseguono il trattamento) in merito agli obblighi derivanti dal Regolamento e da altre disposizioni nazionali o europee relative alla protezione dei dati, sorvegliare l'osservanza del Regolamento e delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali (comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo), fornire - se richiesto - un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento, cooperare con l'Autorità garante per la protezione dei dati personali e fungere da punto di contatto con tale Autorità per questioni connesse al trattamento (es. per la consultazione preventiva di cui all'articolo 36 del Regolamento).
5. I dati di contatto del DPO dovranno essere pubblicati dal Titolare o dal Responsabile del trattamento (in modo che gli interessati possano contattarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti) e comunicati all'Autorità garante per la protezione dei dati personali.

Le misure di sicurezza del nuovo Regolamento europeo

Dott. Lino Fornaro - *Comitato Direttivo Clusit*

Lo scorso 24 maggio è entrato in vigore il nuovo Regolamento Europeo sulla protezione dei dati personali, destinato a rimpiazzare l'ormai datato D.Lgs. 196/03 (Codice in materia di protezione dei dati personali), e che diventerà effettivo dal 25 maggio 2018.
Per due anni, quindi, saranno in vigore due norme, quella italiana e quella europea, ma le sanzioni del nuovo Regolamento saranno applicabili dopo il 25 maggio 2018.
La prima novità che mi preme sottolineare è la natura giuridica di questa norma in quanto un "regolamento europeo", come si dice in gergo, è "self executive", cioè diverrà effettivo senza alcun passaggio parlamentare (non c'è quindi da sperare in proroghe dell'ultimo minuto).
Molti dei principi che ritroviamo in questo Regolamento erano già presenti nella vecchia direttiva UE (la privacy by default, ad esempio, fa pensare al "principio di necessità" già disciplinato dal D.Lgs. 196/03), ma sono stati enfatizzati e rafforzati.
Basti pensare alle novità presenti nelle misure riguardanti la trasparenza del trattamento, la gestione dei consensi, il controllo sui propri dati, il diritto all'oblio, il diritto alla portabilità dei dati, etc.
Passando all'esame delle misure di sicurezza introdotte, il cambio di marcia è ancora più evidente: **scompaiono le vecchie "misure minime" di sicurezza, ormai anacronistiche, e si passa a un approccio sistemico alla sicurezza e alla protezione del dato incentrato sulla risk analysis**, fino a prevedere per taluni trattamenti una preventiva "valutazione d'impatto" (PIA) che non rientra nella trattazione di questo articolo.
Questo importante cambiamento era auspicabile, oltre che scontato, se pensiamo a quanto sia cambiato nell'ultimo decennio il contesto e le modalità con cui vengono trattate le informazioni, con l'evoluzione delle tecnologie a disposizione e la pervasività degli strumenti generalmente utilizzati.
Sono aumentati di pari passo, aggravandosi, i rischi connessi al trattamento dei dati personali, dal furto di identità alla perdita di reputazione, dalle frodi alla negazione dell'accesso ai nostri stessi dati presi in ostaggio da c.d. "cybercriminali" con richieste di "riscatto" da pagare in moneta elettronica (bitcoin).
Alla base c'è l'annoso problema della consapevolezza del valore delle informazioni che trattiamo e dell'inconsapevolezza, di contro, dei rischi cui siamo esposti o a cui esponiamo le informazioni.
Purtroppo, come sempre, c'è chi invece comprende il valore delle informazioni molto più di chi le possiede, e ne fa un business, illecito, ma molto profittevole.
Di fronte a questa situazione, che ho banalizzato per necessità redazionali, per contenere i rischi legati al trattamento delle informazioni riferite alle persone fisiche all'interno dell'Unione, le autorità garanti europee con questo Regolamento impongono ai titolari del trattamento, allorché si accingano a iniziare o a progettare un trattamento di dati personali, di effettuare una seria valutazione e determinare misure adeguate a contrastare i rischi che il trattamento comporta, puntando all'efficacia delle misure e responsabilizzando i titolari dei trattamenti.
Difatti, l'art.32, che titola "Sicurezza del trattamento", così recita:
"1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."
Analizzando il testo di questo articolo, il richiamo alla risk analysis è esplicito, così come espliciti sono gli elementi minimi da tenere in considerazione, tra i quali oltre allo "Stato dell'arte" e "alla natura, all'oggetto e alle finalità del trattamento" che erano in qualche modo richiamati nel vecchio art. 31 del D.Lgs. 196/03, compaiono "i costi di attuazione".
Il richiamo ai costi dà una forte connotazione di business a questo approccio, in quanto richiama il principio che **il "costo della sicurezza" deve essere proporzionato al "valore" del bene o dell'informazione da proteggere**.
Ed è un passaggio molto delicato, perché richiede una corretta valutazione, di contro, dei "costi dell'insicurezza" che purtroppo i nostri imprenditori hanno dimostrato di non essere così abili a calcolare, il che rischia di portare a conclusioni non esattamente in linea con gli obiettivi prefissati (proteggere adeguatamente le informazioni).
Continuando la lettura dell'articolo, al titolare del trattamento viene quindi richiesto di mettere in atto "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*"; per questo il ricorso agli standard come la **ISO 31000** nell'effettuare una risk analysis è quanto mai auspicabile.
Venendo alle misure richieste (*tra le altre, se del caso*) la prima, più volte richiamata nel Regolamento è *la "pseudonimizzazione e la cifratura dei dati personali"*,

dove per **pseudonimizzazione** il Regolamento intende **"***il trattamento di dati personali in modo tale che i dati personali non possano essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*".
È una misura che mira a "depotenziare" il dato, a ridurre cioè in maniera significativa la pericolosità intrinseca dell'informazione (si pensi ai dati sanitari). Se quindi l'informazione, per qualsiasi causa, perde la sua caratteristica di riservatezza, le conseguenze sui diritti e le libertà delle persone non sono compromesse.
Attenzione che le due misure sono sostanzialmente diverse tra di loro perchè **con la cifratura il dato può essere completo ma "incomprensibile", mentre con la pseudonimizzazione non si realizza l'associazione tra la parte di informazione che lederebbe i diritti e le libertà delle persone e il dato identificativo** (la persona a cui appartengono quelle informazioni). Capite bene che non si tratta di dati anonimi, ma di dati per i quali le due parti di informazioni sono state separate e la validità di tale soluzione è direttamente proporzionale alla difficoltà di riunire i due pezzi di informazioni, cioè al "costo" di tale operazione: più è complesso e costoso, in termini di tempo e di effort, più la pseudonimizzazione è da ritenersi forte e quindi in taluni casi accettabile.
In merito alla cifratura, ritenuta la soluzione preferibile, è opportuno tenere ben presente le diverse modalità con cui questa è realizzabile, le diverse tecnologie - quali ad esempio la cifratura del supporto (hard disk, chiavetta, etc.), o la cifratura del database, o anche la cifratura del singolo file - e le diverse criticità di ciascuna forma di cifratura. La cifratura del disco, ad esempio, mette al riparo l'informazione quando il disco non è in utilizzo, quindi ad esempio a computer spento, ed è utile contro i furti (a computer acceso i dati sono in chiaro per tutti coloro che vi hanno accesso), al contrario, la cifratura del file è direttamente legata all'informazione e può essere trasportata anche su canali non sicuri, essendo stata cifrata direttamente l'informazione.
Purtroppo non è sempre facile applicare forme di cifratura legate al file, sia perché spesso i dati non sono semplicemente organizzati sotto forma di file (si pensi ai dati sanitari all'interno di applicazioni e database), sia per i problemi di usabilità che la cifratura porta con sé.
Attenzione quindi a valutare bene le soluzioni a seconda dei contesti e delle necessità di protezione e usabilità.
L'usabilità è una componente fondamentale quanto le misure di sicurezza, perché una cattiva "user experience" indurrà l'utilizzatore a ricercare alternative più semplici per la gestione quotidiana del dato, in barba alle policy e agli strumenti messi a disposizione dal titolare.
Continuando la lettura dell'art.32, la misura di sicurezza al punto b) richiede "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"*, dove per resilienza si può intendere la capacità di adattamento a condizioni d'uso e resistenza a situazioni avverse per garantire la disponibilità dei servizi erogati.
Le cause che possono determinare situazioni avverse possono essere ricondotte a un guasto tecnico, all'errore umano, a un disastro naturale, al vandalismo, all'intrusione informatica o all'azione di un malware. Prendendo in esame anche il contenuto della successiva misura di sicurezza presente nel punto *c), "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico"*, si comprende come la portata delle misure richieste è ben lontana dalle vecchie misure minime di sicurezza, ma è più orientata a processi e soluzioni che hanno come riferimento la Business Continuity (attenzione, non è obbligatorio un piano di BC/DR), e ancor prima all'esigenza di mettere in campo procedure e strumenti per rispondere agli incidenti (incident response).

Il paragrafo 1 dell'art. 32 si chiude con la lettera *d)* che richiede *"una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"*.
Quest'ultimo punto toglie ogni dubbio residuo rispetto all'approccio richiesto nella gestione della sicurezza delle informazioni da questo Regolamento, **un approccio orientato ai processi**, in un ciclo di miglioramento continuo nel quale vengono regolarmente valutate - ed eventualmente corrette - le misure o i controlli adottati per mitigare i rischi del trattamento.
Altra novità di rilievo in questo Regolamento è quella che riguarda l'obbligo di **denuncia alle autorità dei Data Breach**, obbligo che era stato anticipato dal Garante italiano per gli operatori di servizi di telecomunicazione.
Questo intervento va nella direzione di estendere alle imprese e alle Pubbliche amministrazioni tale obbligo, e di abbattere la resistenza delle imprese a denunciare le violazioni subite, oltre che indurle a dotarsi di strumenti che consentano loro di rilevare le intrusioni (altrimenti come farebbero a denunciarle?).
È un passaggio molto importante, soprattutto di tipo culturale, perché esiste il giustificato timore dell'imprenditore nel denunciare una violazione, soprattutto per la possibile ricaduta negativa in termini di immagine che avrebbe l'azienda nel caso in cui la notizia diventasse di pubblico dominio: questo atteggiamento non fa che favorire i cybercriminali.
Invece, la condivisione delle informazioni relative agli attacchi subiti e alle modalità con cui questi attacchi sono stati condotti, andando o meno a buon fine, non può che iniziare a creare un meccanismo virtuoso che col tempo aiuterà a limitare il numero delle vittime di attacchi "seriali", aiutando il sistema a imparare e a limitare o impedire che lo stesso tipo di attacco possa essere ripetuto su ampia scala. Ma prima di arrivare a tanto, tale condivisione sarebbe già un grosso successo se servisse anche solo a rendere coscienti gli imprenditori dell'effettività e della pericolosità del cybercrime.

Tornando al testo della norma, è l'art. 33 a regolamentare la denuncia dei cd Data Breach e a imporre al titolare del trattamento di effettuare la notifica della violazione all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, indicando al paragrafo 3 i contenuti minimi della notifica (si rimanda alla lettura dell'art.33 per i dettagli).
È importante sottolineare che il paragrafo 5 dell'art.33 impone la tenuta di un registro delle violazioni dei dati personali nel quale documentare anche le circostanze, le conseguenze e i provvedimenti adottati per porre rimedio alla violazione.
Ma se è vero che il timore di ripercussioni di immagine induce gli imprenditori a non denunciare alle autorità le violazioni subite, non piacerà affatto sapere che l'art.34 in taluni casi li obbliga a **notificare la violazione subita non solo all'autorità, che ne garantisce la riservatezza, ma anche gli interessati**, come si legge al par.1. "*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo*". L'unica via di fuga la riserva il paragrafo 3 dell'art.34 che alla lettera *a)* individua nella cifratura una misura idonea a scongiurare l'obbligo di notifica agli interessati mentre alla lettera *c)* dello stesso articolo, lì dove la comunicazione ai singoli interessati richiederebbe sforzi sproporzionati, prevede il ricorso "[…] *a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia*".
A fronte di questa prospettiva, le organizzazioni, pubbliche o private che siano, farebbero bene ad adottare opportune strategie di comunicazione per limitare l'eventuale danno di immagine che potrebbe derivare dal ritrovarsi nella condizione di dover effettuare una comunicazione pubblica o anche solo diretta agli interessati, in merito a una violazione subita, alla stregua di quanto generalmente avviene per le grandi organizzazioni all'interno di un più ampio contesto di crisis management.

Dalla Direttiva 99/93/CE al Regolamento eIDAS: come cambiano le nostre firme elettroniche

Avv. Luigi Foglia - *D&L Department - Studio Legale Lisi, esponente del consiglio direttivo ANORC*

Dal primo luglio 2016 è stata definitivamente abrogata la direttiva europea 1999/93/CE che ha rappresentato, fino a ieri, il quadro comunitario in tema di firme elettroniche.
La direttiva, che ogni singolo stato ha provveduto negli anni a recepire nel proprio ordinamento, pur ponendosi degli obiettivi meritevoli, non è stata in grado, per l'eccessiva frammentazione e diversità dei singoli ordinamenti nazionali, di creare un quadro giuridico comune che fornisse terreno fertile alle transazioni transfrontaliere.
Prendendo atto di tali limiti, nel maggio 2011 il Consiglio dell'Unione Europea ha invitato la Commissione europea a contribuire al mercato unico digitale creando le condizioni adatte per il riconoscimento reciproco transfrontaliero di funzioni essenziali quali l'identificazione elettronica, i documenti elettronici, le firme elettroniche e i servizi elettronici di recapito, nonché per l'interoperabilità dei servizi di eGovernment in tutta l'Unione europea. Anche il Parlamento europeo, nella risoluzione del 21 settembre 2010 sul completamento del mercato interno per il commercio elettronico, ha sottolineato l'importanza della sicurezza dei servizi elettronici, in particolare delle firme elettroniche.
In tale ottica, quindi, è stato emanato il Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio dell'Unione europea del 23 luglio 2014, che ha compiutamente regolamentato non solo le firme elettroniche ma anche altri servizi fiduciari per le transazioni elettroniche nonché l'identificazione elettronica.
Occorre ricordare che il Regolamento, diversamente dalla Direttiva, non deve essere recepito da ogni singolo Stato membro ma risulta immediatamente cogente e prevalente in caso di contrasto con la normativa interna. Proviamo, quindi, a soffermarci sulle **principali novità in tema di firme elettroniche introdotte dal Regolamento e sul loro possibile impatto sulla normativa italiana**.
Innanzitutto, è utile ripercorrere brevemente la travagliata storia delle firme elettroniche in Italia. A seguito dell'approvazione della direttiva 99/93/CE, infatti, l'Italia ha introdotto nel nostro ordinamento (dove, giova ricordarlo, già il DPR 513 del 10 novembre 1997 riconosceva valore giuridico alla firma digitale) i concetti di firma elettronica e di firma elettronica avanzata (con il D.Lgs. 23 gennaio 2002, n.10) e di firma elettronica qualificata (inquadrando la firma digitale in tale tipologia di firma con il DPR 7 aprile 2003, n.137). A riprova, però, delle difficoltà incontrate da ogni singolo stato membro nell'applicazione della direttiva, con il D.Lgs. 82/2005 (che ha introdotto nel nostro ordinamento il Codice dell'amministrazione digitale) è scomparsa tra le firme elettroniche la firma elettronica avanzata che è stata poi reintrodotta (e finalmente regolamentata con il DPCM 22 febbraio 2013) solo con le modifiche al CAD avutesi con il D.Lgs 30 dicembre 2010, n. 235.
Il quadro giuridico che vien fuori da questo stratificarsi di normative successive è contenuto negli artt. 21 e seguenti del CAD in base ai quali, in estrema sintesi, viene lasciata libertà al giudice di riconoscere il valore giuridico dei documenti sottoscritti con firma elettronica "semplice" (una firma che, quindi, non soddisfi i requisiti previsti per le firme avanzate o per quelle qualificate o digitali) sulla base dei parametri legati a qualità, sicurezza, integrità e immodificabilità del suo contenuto informativo. Diversamente, ai documenti sottoscritti con firme avanzate, qualificate o digitali, viene riconosciuta la forma scritta e il valore giuridico che l'art. 2702 del codice civile riconosce alle scritture private.
Il regolamento eIDAS, invece, in tema di firme elettroniche stabilisce in via generale che "*ad una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova* in procedimenti giudiziali per il sol motivo della sua forma elettronica o perché non soddisfa i requisiti per le firme elettroniche avanzate" (art. 25 del Regolamento).
Tuttavia, spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatta salva la firma elettronica qualificata, alla quale è riconosciuto da ogni stato membro il medesimo valore giuridico (e i medesimi effetti) attribuito alla sottoscrizione autografa (considerando 49 e art. 25 del Regolamento).
Come risulta evidente da una lettura comparata degli artt. 25 e seguenti del Regolamento eIDAS e degli articoli 21 e seguenti del CAD, mentre il Regolamento si occupa di firme, il CAD ruota intorno al valore giuridico e probatorio del documento informatico sottoscritto con le differenti tipologie di firme elettroniche riconosciute (semplice, avanzata, qualificata e digitale).
Se, infatti, in sede comunitaria non si è raggiunta un'univoca visione in tema di documento informatico (a dire il vero il Regolamento parla di documento elettronico), si è comunque imposto un quadro comune almeno in tema di firme elettroniche.
Il Regolamento, infatti, ha individuato (potremmo dire anche "ricordato", in quanto non ci sono variazioni rispetto

alla precedente direttiva 99/93/CE) **i requisiti minimi che devono essere soddisfatti da una firma elettronica perché essa possa essere considerata avanzata**: "*a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati*".
Accanto a tali requisiti, però, la normativa non individua un valore giuridico comune, lasciando libero ogni stato membro di regolamentarsi in maniera differente (eccezion fatta, come abbiamo visto, per le firme qualificate che risultano parificate alle firme autografe).
In ambito pubblico, però, ove 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 dovrà riconoscere le firme elettroniche avanzate nel caso in cui queste siano state create utilizzando i formati CadES, PadES o XadES - previsti con la Decisione di esecuzione UE 2015/1506 dell'8 settembre 2015 – oppure qualora siano stati comunque resi disponibili, dallo Stato membro in cui è stabilito il prestatore di servizi fiduciari utilizzato dal firmatario, sistemi di convalida della firma realizzati nel rispetto di quanto previsto dalla stessa Decisione di esecuzione.
Il Regolamento individua, poi, i requisiti che devono soddisfare i certificati di firma per essere considerati qualificati e i requisiti e le modalità di certificazione dei dispositivi per la creazione di firme elettroniche qualificate. Le firme elettroniche qualificate, infatti, per poter essere considerate tali, devono soddisfare i requisiti previsti per le firme elettroniche avanzate, essere basate su di un certificato qualificato rilasciato da un prestatore di servizi qualificato ed essere realizzate mediante un dispositivo di firma certificato.
A tal fine il Regolamento prevede l'istituzione, in ogni stato membro, di un elenco di prestatori di servizi fiduciari qualificati e di un elenco dei dispositivi certificati per la creazione di firme elettroniche qualificate.
Inoltre, vengono individuati i requisiti di convalida delle firme qualificate e viene introdotto un servizio ancillare che ha come oggetto proprio la convalida delle firme elettroniche qualificate e che consenta alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in modo automatizzato, affidabile ed efficiente e che rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.
Accanto a tale servizio di convalida è stato anche previsto un ulteriore servizio fiduciario ancillare alle firme elettroniche, che prevede la conservazione delle firme e dei sigilli elettronici qualificati da parte di 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.
Viene quindi migliorato e rinforzato un quadro giuridico comune in tema di firma qualificata e di suo mutuo riconoscimento su tutto il territorio dell'Unione Europea, che rende effettivamente utilizzabili le firme elettroniche qualificate per le transazioni transfrontaliere. Inoltre, mediante accordi che la Comunità europea potrà sottoscrivere con altri stati extracomunitari, tale quadro potrà essere esteso anche al di là dei confini comunitari.
A fronte di tale quadro europeo, il nostro ordinamento non subirà forti impatti, in quanto effettivamente le firme elettroniche attualmente utilizzate in Italia possono essere facilmente riportate all'interno del quadro europeo appena descritto.
Certamente qualche impatto ci sarà in tema di firme elettroniche avanzate che, come abbiamo ricordato, in Italia risultano ulteriormente regolamentate dal DPCM 22 febbraio 2013: **il rischio è che si possa creare un doppio binario (FEA italiana e FEA europea)** laddove la FEA italiana risulterebbe però molto più complessa da realizzare rispetto a quella europea, con innegabile svantaggio per i nostri operatori rispetto a quelli degli altri stati membri.
C'è poi da sciogliere un nodo interpretativo relativo all'art. 3 dell'allegato II del Regolamento (requisiti per i dispositivi per la creazione della firma elettronica qualificata), in base al quale la generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciari qualificato. Ciò sembrerebbe in contrasto con quanto previsto dall'art. 3 comma 4 del DPCM 22 febbraio 2013, in base al quale le firme remote possono essere realizzate mediante dispositivi (HSM) custoditi e gestiti non solo dal certificatore accreditato "*ma anche dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi*".
Il dubbio interpretativo è ancor più forte laddove lo stesso Regolamento, al considerando 51, ritiene che sia opportuno che "*il firmatario possa affidare a terzi i dispositivi per la creazione di una firma elettronica qualificata, purché siano rispettati appropriati meccanismi e procedure per garantire che il firmatario mantenga il controllo esclusivo sull'uso dei suoi dati di creazione di firma elettronica e l'uso del dispositivo soddisfi i requisiti della firma elettronica qualificata*".
Nell'attesa che il legislatore aggiorni il CAD alle nuove definizioni del Regolamento eIDAS e al nuovo quadro di certificazione e accreditamento dei prestatori di servizi qualificati, è utile ricordare che, in via transitoria, nonostante l'abrogazione della direttiva 99/93/CE, viene ancora riconosciuta validità alle firme qualificate basate su certificati qualificati rilasciati da prestatori di servizi qualificati a norma della precedente direttiva. Entro il 1° luglio 2017, però, i certificatori dovranno presentare un'apposita valutazione di conformità che dovrà essere valutata dall'organismo di vigilanza (per l'Italia l'AgID).

Le regole di interoperabilità per le firme elettroniche conformi a eIDAS

Ing. Giovanni Manca - *Presidente ANORC*

Il Regolamento Europeo n. 910/2014 del Parlamento Europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (che abroga la direttiva 1999/93/CE) è applicabile nelle sue parti fondamentali dall'1 luglio 2016.
Tale Regolamento è ampiamente citato mediante l'acronimo eIDAS (electronic IDentification Authentication and Signature) e così vi faremo riferimento in seguito.
È proprio il Legislatore comunitario che spiega perché si è ritenuto opportuno, nell'ambito della creazione di un mercato unico digitale, stabilire un Regolamento sui temi dei servizi fiduciari digitali.
Infatti nella premessa (considerando) n. 3 leggiamo:
"La 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. Il presente regolamento rafforza ed estende l'acquis di tale direttiva".
Il Regolamento eIDAS, composto da 77 "considerando", 52 articoli e 4 allegati modifica profondamente il quadro comunitario in materia di documento elettronico, firme e sigilli elettronici.
Introduce anche i servizi di recapito certificato, simili alla nostra Posta Elettronica Certificata (PEC) e la conservazione di firme, sigilli e certificati digitali. Quest'ultima non è la nostra conservazione digitale di documenti ma ha l'obiettivo di assicurare la verificabilità delle firme e dei sigilli per lunghi periodi.

In questo articolo, stante l'estrema complessità del Regolamento eIDAS, focalizziamo la nostra attenzione sul **mutuo riconoscimento della sottoscrizione elettronica**. In Italia su questo tema ci si esprime in termini di interoperabilità delle firme elettroniche; invece nel Regolamento eIDAS l'interoperabilità si riferisce agli schemi di identificazione elettronica ovvero alla possibilità che un servizio in rete offerto da uno Stato membro sia accessibile con le credenziali digitali emesse da uno o più Stati membri secondo quanto stabilito, ovviamente, nel Regolamento eIDAS in materia di livelli di garanzia della sicurezza delle credenziali e appunto, regole di interoperabilità.
Per l'Italia facciamo riferimento al Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese, ben noto con l'acronimo SPID.
Ma ritorniamo al tema del mutuo riconoscimento della sottoscrizione digitale.
Nel mondo cartaceo si firma secondo le consuete regole culturali già metabolizzate e ben note non appena si impara a leggere e scrivere.
La firma è personale, fortemente associabile al sottoscrittore e in alcuni contesti è obbligatorio produrla in forma "leggibile".
Il mondo digitale è differente. La sottoscrizione è un numero binario prodotto secondo un procedimento informatico che soddisfa alcuni requisiti.
La firma è connessa unicamente al firmatario ed è idonea a identificarlo. Viene creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo. Infine essa è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
L'identità del sottoscrittore è rilasciata da particolari soggetti denominati Prestatori di Servizi Fiduciari (Trust Service Provider) che, quando sono in possesso di specifiche caratteristiche di qualità e sicurezza, possono ottenere l'attributo di qualificati. Per l'associazione dell'identità digitale al titolare vengono utilizzati i cosiddetti certificati digitali e il riconoscimento del titolare stesso è soggetto a stringenti regole per evitare al massimo il rischio di furto di identità.
Il controllo esclusivo del sottoscrittore è garantito da specifici dispositivi per la creazione della firma. Sono ben note le smart card, i token USB che concentrano in un unico dispositivo il chip e il lettore dello stesso. In Italia oltre il 60% dei certificati digitali è disponibile al titolare in modalità remota, ovvero la firma è prodotta tramite un servizio remoto pur essendo soddisfatti i requisiti minimi di sicurezza che il Prestatore qualificato deve garantire.
In questo modo, è possibile generare una firma elettronica qualificata che a livello europeo è equiparata a una sottoscrizione autografa. Gli ordinamenti nazionali (in Italia il Codice dell'amministrazione digitale – CAD) stabiliscono l'efficacia probatoria della sottoscrizione qualificata.
In Italia è possibile utilizzare la firma qualificata (ma anche la firma elettronica avanzata, in particolari condizioni) per sottoscrivere soddisfacendo la forma scritta anche quando essa è obbligatoria.
Ma rimane il problema di riconoscere come valido quel numero (oggi prevalentemente lungo 2.048 bit).
È utile premettere che le regole tecniche italiane per le sottoscrizioni sono superate da quanto stabilito nel Regolamento eIDAS. **La normazione italiana è valida solo se non in contrasto con le regole tecniche europee. Tali regole tecniche sono stabilite dagli organismi di**

standardizzazione di riferimento per l'Europa che sono il CEN e l'ETSI. In tali sedi sono state decise regole tecniche per le strutture dati dei certificati e delle sottoscrizioni digitali. Sono state anche stabilite le regole di sicurezza per i dispositivi di firma.
La Commissione impone l'utilizzo di questi standard tramite i cosiddetti Atti secondari del Regolamento eIDAS: questi sono stati emessi in tempo utile per poter essere applicati entro l'1 luglio 2016 tramite delle Decisioni di esecuzione (implementing acts).
In base a questi standard siamo in grado di produrre firme mutuamente riconoscibili e marche temporali (validazione temporale elettronica qualificata in eIDAS) opponibili ai terzi nell'ambito comunitario.
In verità, i formati delle marche e dei certificati non sono obbligatori ma sarebbe paradossale utilizzare altri formati in modo volontario da parte dei Prestatori. Non avrebbero che svantaggi.
Il quadro comunitario non è esente da potenziali problemi.
Le modalità di riconoscimento del titolare in Italia si sono spinte molto in avanti. Questa fase è cruciale e costosa sul piano organizzativo, infatti, **vista la grandissima emissione di certificati digitali italiani, molti metodi innovativi di riconoscimento (anche da remoto, tramite web cam) sono stati messi in opera**.
Queste tecniche dovranno coordinarsi con le legislazioni nazionali e trovare un ragionevole equilibrio. Per esempio, in alcuni paesi è illegale fare la fotocopia del documento di identità, in altri la firma qualificata è rilasciata direttamente tramite gli sportelli ATM (i Bancomat): **l'analisi del rischio di furto di identità diventa fondamentale**.
Ma tutto ciò premesso, quanto possiamo essere tranquilli sul mutuo riconoscimento di quel famoso numero che sappiamo essere una firma elettronica qualificata?
In Italia non abbiamo problemi particolari, **il mutuo riconoscimento delle sottoscrizioni è stabile e consolidato da oltre 16 anni**.

A livello comunitario ci dobbiamo attenere a quanto stabilito nell'articolo 27 del Regolamento eIDAS.
"Se uno Stato membro richiede 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 formati o utilizzino i metodi definiti negli atti di esecuzione […]".
Inoltre
"*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 […]"*
Vari atti di esecuzione sono stati pubblicati l'8 settembre 2015. Quello da tenere in conto a proposito di quanto descritto nel presente articolo è il 2015/1506.
In esso vengono riproposti i ben noti **formati CAdES, PAdES e XAdES** nelle loro versioni aggiornate.
La novità è una struttura dati per l'aggregazione di dati sottoscritti denominata contenitore con firma associata (Associated Signature Container – AsiC).
Possiamo concludere affermando che il problema del mutuo riconoscimento (interoperabilità) delle sottoscrizioni digitali è certamente da affrontare ma non presenta particolari criticità. Il nostro codice fiscale dovrà confrontarsi con altre realtà europee ma la previsione di un codice europeo già propone ulteriori scenari.
La necessaria e dovuta attenzione e la grande esperienza italiana sulle transazioni sottoscritte digitalmente consentiranno di affrontare e gestire i problemi europei di mutuo riconoscimento delle sottoscrizioni elettroniche con professionalità e adeguata forza risolutiva.

Firma Grafometrica: il futuro si chiama interoperabilità

Proff. Giuseppe Pirlo, Donato Impedovo - *Dipartimento di Informatica dell'Università degli Studi di Bari Aldo Moro. Coordinatori del gruppo di lavoro AIFAG "Test di Conformità alla norma ISO/IEC 19794-7 – full format"*

Con l'aumento e la diversificazione dei servizi online offerti dalle pubbliche amministrazioni e dalle aziende private, negli ultimi anni è sempre più sentita l'esigenza di una identificazione personale semplice e sicura. Il cittadino che si collega alla rete per poter fruire di servizi amministrativi o sanitari, o anche per poter accedere a siti di e-commerce e bancari, deve innanzitutto essere identificato con certezza. Nessuno di noi accetterebbe mai che fosse possibile a una persona diversa da noi stessi accedere a informazioni sul nostro conto corrente bancario e magari anche potervi agire.

In passato i meccanismi tradizionali per riconoscere automaticamente un individuo si sono basati sul possesso di oggetti fisici (es. chiavi o badge) o sulla conoscenza di informazioni riservate (es. password). Quando preleviamo contante con il bancomat utilizziamo in realtà sia un oggetto fisico, la nostra tessera bancomat, che una informazione riservata, il nostro Personal Identification Number (PIN). In realtà con l'aumento dei siti e delle applicazioni per le quali siamo chiamati ad autenticarci, ognuno di noi deve conoscere già molte password a volte difficili da ricordare e spesso facili da ricostruire da parte di malintenzionati.

È facile, quindi, comprendere come la biometria sia diventata ultimamente campo di grande interesse sia da un punto di vista scientifico e tecnologico che da un punto di vista applicativo e commerciale. **Con le tecniche biometriche l'identificazione personale si basa sulle caratteristiche fisiche o comportamentali dell'individuo, caratteristiche che non possono essere rubate, perdute o dimenticate**. Tra le numerose caratteristiche biometriche, la **firma grafometrica** sta ricevendo specifica attenzione in quanto è giustamente considerata strumento abilitante e di semplificazione per accedere a servizi online. Inoltre, la firma grafometrica, che formalmente è una particolare tipologia di Firma Elettronica Avanzata (FEA), può essere apposta da un individuo esattamente nello stesso modo con il quale egli firma un documento cartaceo, e questo è considerato un elemento fondamentale in quanto non richiede specifiche competenze da parte dell'utente e rende la firma grafometrica accettata con grande naturalezza. La firma grafometrica può inoltre essere apposta su tavolette elettroniche ma anche su dispositivi mobili come tablet e smartphone. **Essa quindi contiene sia informazioni statiche legate all'immagine della firma, che informazioni dinamiche legate al processo di apposizione**, come la velocità di scrittura, l'accelerazione e la pressione della penna sul dispositivo. L'insieme di queste informazioni consente, come dimostrano le ricerche più avanzate in questo settore, non solo di verificare l'identità del firmatario, ma anche di derivare informazioni legate al suo stato fisico e psicologico. Con la firma grafometrica, inoltre, il documento viene firmato senza mai doverlo stampare su carta, con grande risparmio di tempo e senza spreco di carta. Ovviamente, per poter utilizzare questo strumento straordinariamente flessibile e potente **è necessario che lo si implementi in maniera tale da garantire il suo funzionamento indipendentemente dal dispositivo utilizzato** per l'acquisizione della firma stessa. In altre parole, l'utente deve poter apporre la propria firma su un tablet o sulla tavoletta elettronica di un ufficio pubblico, o ancora deve poter effettuare una transazione bancaria firmando la documentazione dal suo smartphone personale senza nessuna limitazione. In realtà dispositivi differenti, realizzati da produttori diversi o che utilizzano tecnologie diverse, possono rilevare i segnali del processo di scrittura in maniera non perfettamente uguale e quindi **le soluzioni di firma realizzate finora sono per lo più legate a uno specifico dispositivo, non sono cioè interoperabili**. È la soluzione tecnologica che deve risultare interoperabile, ovvero perfettamente funzionante indipendentemente dal dispositivo utilizzato per l'acquisizione della firma.

Un passo fondamentale verso l'interoperabilità della soluzione di firma grafometrica è stato compiuto con la definizione di uno specifico standard di formato dei dati. Lo standard **ISO/IEC 19794-7:2014** indica le specifiche per l'interscambio di firme tra diversi sistemi. Allo stato attuale non esiste uno strumento che consenta di verificare automaticamente e certificare che il tracciato generato da una soluzione per l'elaborazione della firma grafometrica sia conforme a tale standard. **L'AIFAG ha intercettato tale mancanza istituendo un gruppo di lavoro che ha avuto l'obiettivo di verificare l'aderenza allo standard di tracciati di firma generati da sistemi commerciali e allo stesso tempo di misurare il loro livello di compatibilità**.

Il gruppo di lavoro ha elaborato e implementato uno specifico protocollo per le analisi. In una prima fase le aziende hanno generato dei file contenenti le firme per

mezzo dei rispettivi software, successivamente tali file sono stati anonimizzati e re-inviati a tutte le aziende al fine di verificare: l'accessibilità ai file in termini di importazione; il formato importato; l'aderenza dei dati contenuti ai requisiti della norma. I requisiti oggetto di verifica hanno riguardato le dimensioni, la data, la tecnologia di acquisizione, i valori dei canali e i loro attributi (da R-11 a R-56). Inoltre sono stati estratti anche i valori dei canali e si sono ricostruite le immagini firma partendo dai canali X e Y. Il test così implementato è stato rivolto all'analisi di compatibilità, alla verifica incrociata dei requisiti, alla verifica di confronto con algoritmi automatici tra i campioni dei diversi canali. Il test è stato svolto in modalità anonima con la conoscenza (ai soli coordinatori) della "verità a terra", intesa come reale contenuto dei file di origine.

I risultati del test sono stati presentati nel corso del convegno AIFAG tenutosi il 24 giugno 2016 a Lecce. **In prima istanza, si è osservato come i tracciati generati dalle soluzioni aziendali risultino essere diversi tra loro rispetto alla estensione dei file in cui erano contenuti** (iso19714, bin, hex e dat), ciò ha determinato in fase di analisi la necessità di conversione di formato che ha, in alcuni casi, introdotto errori nella sequenza dei dati. Un ulteriore elemento osservato è che, sebbene lo standard contempli diversi campi, gli stessi non sono sempre popolati (es. tecnologia, marca e modello del dispositivo di acquisizione).

Nelle fasi di apertura/importazione di un tracciato da parte di sistemi terzi, **si sono riscontrati errori principalmente riconducibili a errato popolamento di alcuni campi, errori di rappresentazione e di codifica**. I tracciati sono stati importati con successo solo a seguito di adattamenti, conversioni o modifiche, tuttavia **si è osservato come nell'80% dei casi gli errori rilevati dalle diverse aziende coincidano**. Una analisi numerica sulla sequenza di dati ha rilevato errori compresi tra l'8% e il 16% solo su 3 dei 56 requisiti presi in considerazione.

La fase successiva ha riguardato una ispezione visuale delle firme generate a partire dalle coordinate X e Y estratte dai file. In alcuni casi, la presenza di campioni spuri già presenti nella sequenza di origine o introdotti in fase di conversione porta a una ricostruzione non perfetta del tracciato rispetto a quello di origine e in generale non superiore allo 0,2%. Va tuttavia sottolineato come l'errore debba essere assolutamente nullo.

In conclusione, il test ha evidenziato una attuale non piena compatibilità tra i sistemi presi in esame, tuttavia la distanza tra quanto implementato dai sistemi commerciali e lo standard è risultata essere molto limitata.

La firma grafometrica rimane quindi una tecnologia matura ma che ancora necessita di specifico approfondimento in termini di conformità allo standard. **Il ruolo di AIFAG è quindi quello di continuare a favorire**, attraverso l'indispensabile raccordo tra gli aspetti legati alla normativa e al mercato e quelli tecnologici e scientifici, **che la firma grafometrica diventi realmente quello straordinario strumento abilitante allo sviluppo sociale ed economico del nostro Paese**.

Know IT è la nuova piattaforma di formazione e informazione dedicata ai professionisti dell'era digitale. Il percorso di digitalizzazione, anche se a piccoli passi, sta rivoluzionando gli scenari di mercato, aprendo nuove prospettive e nuove criticità per la privacy, il commercio elettronico, il diritto d'autore e per la conversione in digitale di processi prima analogici, come la fatturazione, la gestione documentale, la firma. Tutto ciò avrà un impatto sempre maggiore su molti aspetti organizzativi, coinvolgendo PA, aziende, professionisti e cittadini.

Know IT si propone di diffondere una conoscenza digitale che si allarghi dall'area prett amente tecnica a quella normativa e gestionale, implementando la capacità degli utenti di valutare e condurre i nuovi processi e modelli organizzativi, ottimizzandoli e fornendo valore aggiunto al contesto in cui si trovano a operare.

Il nostro programma formativo affronta in particolare le seguenti macrotematiche: e-commerce, diritto d'autore, privacy e sicurezza, firme elettroniche e biometria, e-government, e-health, document management e, in generale, tutti i principali aspetti dell'ICT law.

Corsi on demand dedicati a PA, aziende e professionisti

SCOPRI L'OFFERTA FORMATIVA

www.knowit.clioedu.it

Digital & Law Department
www.studiolegalelisi.it

CLIOEDU®