I QUADERNI DI
Telèma

Uno, nessuno e centomila:
verso una gestione unitaria dell'identità digitale

Carpineto, Castrucci, Guida
Pellegrini, Romano

La diffusione di Internet ha creato una situazione senza precedenti nella quale un numero enorme di transazioni che richiedono qualche processo d'identificazione vengono fatte a distanza mediante l'uso di un browser Web. Attualmente però l'identificazione dell'utente viene generalmente gestita dal software dello specifico fornitore di servizio e l'intero sistema è soggetto a duplicazioni, inefficienze e mancanza di garanzie in termini di sicurezza e privacy. È opinione diffusa che con identificazioni elettroniche più sicure e semplici sarebbe possibile sviluppare servizi online a valore più elevato, riducendo al contempo i costi e aumentando la produttività del settore pubblico.

Nel mondo informatico ci si è pertanto focalizzati sullo sviluppo di sistemi di gestione dell'identità digitale per descrivere in modo univoco un'entità (persona o organizzazione) e consentirle un accesso globale a servizi rilasciati previa autenticazione (ad esempio mediante password). Come vedremo in questo articolo, mentre le soluzioni tecniche sono già sostanzialmente disponibili, la costruzione di un sistema di gestione dell'identità digitale condiviso ed efficace è un processo in itinere che i singoli Paesi stanno cercando di favorire con opportune strategie. Il problema dell'identificazione personale sicura e universale è molto importante ma è soltanto un aspetto dell'identità digitale in senso esteso. Questa si configura come un'incessante accumulazione di informazioni, connessioni, indirizzi, preferenze, appartenenze, interessi condivisi e relazioni generate quotidianamente in un processo non dissimile da quello con cui costruiamo la nostra identità offline. Il diritto all'oblio, così come il diritto di controllare la propria reputazione online e di intervenire nel caso in cui la si ritenga lesiva della propria immagine e della propria persona, rispondono così al crescente bisogno di tutela delle persone nel libero esercizio di costruzione della propria identità digitale, peraltro sempre più sovrapponibile e integrata con la propria identità tout court.

Supplemento al numero 296 di
MEDIA DUEMILA
Ottobre 2013

I QUADERNI DI Telèma

Nei numeri precedenti

IL QUADERNO DI TELÈMA È STATO REALIZZATO DALLA FONDAZIONE UGO BORDONI

Presidente: **Alessandro Luciano** | Direttore delle Ricerche: **Mario Frullone**
Autori del Quaderno: **Carpineto C., Castrucci R., Guida F., Pellegrini M., Romano G.**

Un modello federato di gestione dell'identità digitale

La filosofia dei sistemi di gestione dell'identità digitale è quella di concepire l'autenticazione come un servizio svolto da terze parti, sollevando i Webmaster dalla necessità di fornire il proprio specifico metodo e aiutando gli utenti a consolidare la propria identità digitale. Nei modelli di gestione dell'identità centralizzati, ad esempio quelli che utilizzano carte d'identità elettroniche, è spesso necessario creare e manutenere un registro nazionale e strutture dedicate. In un modello di gestione dell'identità federato si cerca invece di far leva sulle tecnologie e le industrie presenti sul mercato per ottimizzare flessibilità, costi e innovazione, lasciando alle organizzazioni che partecipano alla federazione un elevato grado di autonomia rispetto alle soluzioni tecniche e alle misure da adottare per la sicurezza e la privacy.

Gli attori principali di un modello federato sono i seguenti:

- Gli utenti muniti di Web browser.
- I fornitori di servizi (chiamati anche relying parties): sono i siti Web che richiedono credenziali di sicurezza dagli utenti.
- I fornitori d'identità: sono i siti Web che forniscono le credenziali di sicurezza ai fornitori di servizi su incarico degli utenti. Tali credenziali di sicurezza possono contenere attributi (claims) quali nome, indirizzo, età, ecc.

Per implementare un modello federato sono possibili varie soluzioni tecniche quali, ad esempio, OpenID, OAuth, Information Cards. In questo articolo faremo riferimento a OpenID, uno standard aperto che ha avuto una grande diffusione e, in alcuni Paesi, è diventato uno dei pilastri delle strategie di gestione dell'identità digitale. Il modello è visualizzato in Figura 1. Si assume che l'utente abbia preliminarmente effettuato una registrazione OpenID presso uno dei vari fornitori d'identità OpenID e che, successivamente, cerchi di accedere ad un sito o applicazione che fornisce un servizio ad utenti registrati. Il flusso delle informazioni viene scandito dalla numerazione delle frecce, dove ciascuna freccia corrisponde alle seguenti azioni:

1) L'utente interagisce con un fornitore di servizio che consente di autenticarsi tramite OpenID e specifica il proprio identificativo OpenID.

2) Il fornitore di servizio contatta il fornitore appropriato d'identità OpenID chiedendogli di verificare l'identità dell'utente.

3) Il fornitore d'identità OpenID chiede all'utente di autenticarsi ed eventualmente di acconsentire a rilasciare altre informazioni richieste dal fornitore di servizio.

4) L'utente invia le credenziali OpenID e l'eventuale consenso.

5) Il fornitore d'identità conferma l'identità dell'utente al fornitore di servizio e gli trasmette le eventuali informazioni aggiuntive.

6) A questo punto il fornitore di servizio consente all'utente l'accesso.

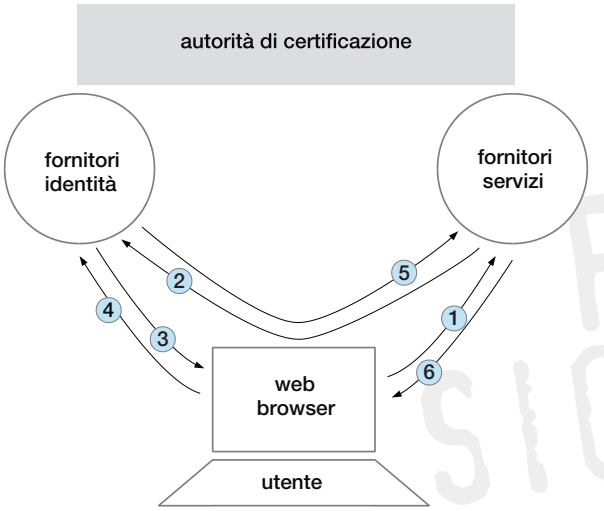

Figura 1. Architettura di un modello federato di gestione dell'identità digitale.

Si noti che il protocollo OpenID non vincola all'uso di una specifica tecnica di autenticazione: gli approcci possibili variano dalla password alle smart card alle tecniche biometriche. Inoltre, per tutelare la privacy, OpenID supporta la generazione di identificativi pseudo-anonimi mediante i quali lo stesso utente può adoperare identificativi diversi quando passa da un sito all'altro. Bisogna considerare inoltre che i fornitori d'identità OpenID sono tipicamente grandi organizzazioni specializzate nella gestione sicura delle identità online (Google, Yahoo!, AOL, ecc.).

Un modello di questo tipo comporta alcuni evidenti vantaggi per l'utente, richiedendogli di gestire un minor numero di credenziali e facilitando la registrazione sui siti mediante popolamento automatico con le informazioni base del profilo (nome, data di nascita, indirizzo).

D'altra parte, se in teoria lo schema appena illustrato garantisce la possibilità tecnica della registrazione via terze parti, in pratica esso non è sufficiente affinché questa modalità si affermi e diventi d'uso comune. L'intero sistema deve guadagnare credibilità e fiducia agli occhi dei soggetti che erogano servizi su Internet. Nell'industria delle carte di credito, ad esempio, è passato molto tempo dalla standardizzazione dei lettori allo sviluppo del mercato. Soltanto quando sono nate delle grandi reti di carte di credito, i commercianti si sono convinti che una particolare carta di credito emessa da una banca era affidabile.

Nel nostro caso, non basta installare nuovo software sui siti governativi. Occorre invece incentivare la fiducia nelle credenziali emesse dai fornitori d'identità (terze parti commerciali, accademiche, no-profit) con i quali il governo non ha un rapporto diretto. Per consentire un'evoluzione di questo tipo, la strategia più efficace sembra quella di affidarsi ad autorità certificatrici. Questo è il quarto attore del modello, coincidente con lo strato superiore della Figura 1, e sembra determinante per il suo successo.

La struttura e il funzionamento delle autorità certificatrici possono, a loro volta, diventare alquanto complessi. In uno schema semplificato, possiamo prevedere innanzitutto che i decisori politici ed economici stabiliscano sulla base delle normative vigenti i requisiti di sicurezza e privacy che devono possedere i fornitori d'identità per raggiungere un adeguato livello di garanzia. Analoghi requisiti potranno riguardare in alcuni casi le misure per la protezione dei dati gestiti dai fornitori d'identità e dai fornitori di servizi. Oltre a stabilire detti requisiti, bisognerà specificare chi controllerà che saranno rispettati. Questa funzione potrà essere svolta da valutatori qualificati (enti o persone) che hanno una determinata esperienza professionale. A questo punto, sarebbe compito di un'autorità certificatrice realizzare un programma di certificazione nel quale:

- vengono create e pubblicizzate le liste dei valutatori;
- vengono create e pubblicizzate le liste degli enti accreditati (sia fornitori d'identità sia, in qualche caso, fornitori di servizi);
- le liste vengono rinnovate periodicamente.

L'insieme di queste attività di certificazione è detto "trust framework". Negli Stati Uniti, in particolare, sono state attivate varie iniziative che mirano a realizzare un trust framework, come spiegato meglio in seguito.

Problematiche nella gestione delle identità digitali

Cerchiamo ora di capire meglio quali sono gli interessi di ciascun attore coinvolto nel modello federato, perché il loro soddisfacimento condiziona le modalità di accreditamento e i requisiti organizzativi delle entità coinvolte.

Utenti:

1. Semplicità nel provare la propria identità:

- poche credenziali da conservare per accedere ad una pluralità di servizi (ha però come contropartita l'accesso illecito a molti servizi in caso di compromissione delle credenziali);
- utilizzo agevole di eventuali tecniche di riconoscimento non basate sulla conoscenza di password (ad esempio dispositivi aggiuntivi non necessari o facilmente ed economicamente reperibili, tecniche di riconoscimento biometrico che non provochino attese significative e/o preoccupazioni).

2. Semplice e indisturbata fruizione dei servizi:

- comunicazione dati personali solo nei casi in cui la maggiore semplicità non sia pesantemente pagata in altri termini (ad esempio inserzioni pubblicitarie martellanti).

3. Elevata sicurezza (normalmente in contrasto con il punto 1), per minimizzare il rischio di danni (ad esempio addebiti illeciti).

4. Diritto all'oblio e tutela della reputazione.

Fornitori di servizi:

1. Diffusione dei servizi e conseguente co-interesse nel soddisfare le esigenze dell'utente, quando non contrastanti con le proprie.

2. Elevata sicurezza, ma con contromisure finalizzate a tutelare in primo luogo i propri interessi (ad esempio fatturazione, contrasto dell'utilizzo abusivo dei servizi, ecc.) e, in seconda battuta, quelli dell'utente quando indirettamente coincidenti con i propri (vedi punto 1).

3. Scambio a scopo di lucro con altri fornitori di servizi e/o d'identità di parte delle informazioni dell'utente diverse da quelle necessarie per l'accesso ai servizi (ad esempio relative ad azioni e comportamenti dell'utente durante l'utilizzo dei servizi).

Fornitori d'identità:

Vale quanto detto per i fornitori di servizi, in quanto anche la fornitura delle identità è un servizio.

Autorità di certificazione:

Possono essere commerciali, istituzionali o agenti per conto di istituzioni (gestori). Nei casi in cui siano soggetti commerciali devono conciliare, per quanto possibile, il ruolo di parte fidata con l'interesse

primario di realizzare utili. Ciò vale anche per i gestori, quando siano organizzazioni commerciali, ma in questo caso vi sono generalmente una serie di condizioni, vincoli e controlli definiti dalle istituzioni per conto delle quali operano. Nel caso in cui le autorità di certificazione fossero invece direttamente gestite da istituzioni, il loro interesse primario sarebbe evidentemente quello di tutelare tutte le entità coinvolte nel modello federato, a partire dall'utente che generalmente rappresenta l'entità più debole. La tipologia (organizzazione commerciale, gestore o istituzione) delle autorità di certificazione dovrebbe essere adeguata alla criticità dei servizi forniti. Il loro ruolo di garanzia è molto importante. In vari modelli di gestione delle identità digitali sono definite su una scala gerarchica diverse entità che, a vari livelli, contribuiscono a fornire le garanzie necessarie per la certificazione.

Stato:

In aggiunta a quanto detto nel caso delle autorità di certificazione istituzionali, si può dire che lo Stato, anche quando non ricopre alcun ruolo nel modello federato, è comunque sempre un'entità da considerare. L'interesse primario può essere quello di vigilare sul rispetto delle norme di legge, in particolar modo prevedendo, ove possibile, controlli sul rispetto della normativa sulla privacy (a tutela degli interessi 2 e 4 dell'utente) e sulla firma elettronica (nei casi in cui venga utilizzata nell'ambito dei servizi forniti). In tale ambito, la complessità è accresciuta dalla distribuzione in Paesi diversi delle entità interagenti e dalla conseguente necessità di fare riferimento anche alla normativa internazionale in tema di privacy e firme elettroniche.

Da quanto detto, risulta evidente che gli interessi in gioco possono essere contrastanti, talvolta anche quando riferiti ad una stessa entità (ad esempio l'utente). A maggior ragione lo sono quando si confrontano gli interessi di diverse entità (ad esempio gli interessi 2 e 4 dell'utente in contrapposizione all'interesse 3 dei fornitori di servizi). La particolare implementazione di un modello federato deve quindi essere in grado di bilanciare i desiderata nel rispetto dei vincoli.

Inoltre, le architetture federate di gestione dell'identità, se applicate a tipologie di servizi non omogenee dal punto di vista della criticità (strettamente legata all'entità dei possibili danni che possono derivare da eventi intenzionali e accidentali), devono poter gestire la sicurezza a vari livelli, prevedendo soprattutto modalità di autenticazione differenziate. Se per talune tipologie di servizi aventi criticità simili il numero di servizi fosse molto limitato, i vantaggi di un'architettura federata sarebbero alquanto limitati.

Identità digitale estesa, tutela della reputazione e diritto all'oblio

La tensione tra la natura processuale dell'identità e la sclerotizzante tendenza del mondo digitale a reificarla nella forma di un insieme crescente di dati è solo uno dei numerosi momenti di frizione tra i diritti connessi all'identità di una persona e i modi di funzionamento dei media digitali. In questo articolo, il problema dell'identità digitale estesa viene affrontato discutendone i due temi chiave del diritto all'oblio e del *reputation management*, in linea con la produzione normativa europea e nazionale, mentre ci si limita ad accennare alla necessità di approfondire la riflessione teorica e giuridica sugli altri aspetti.

Nel mondo digitale, come fuori, la nostra identità si forma da una serie di fattori che riguardano il nostro

corpo, la nostra mente e le nostre relazioni. L'identità digitale estesa è un concetto che prende le mosse da quello di corpo elettronico (Rodotà 2005) che, a sua volta, rinvia a una teoria di derivazione mcluhaniana secondo cui le tecnologie (in generale) e i mezzi di comunicazione (in particolare) estendono i nostri sensi oltre i limiti fisici del corpo in sé (Tursi 2011). Ne consegue che impieghiamo i media anche come veicoli per definire la nostra identità (Bolter e Grusin 2002). Lo stesso McLuhan (1964) coniugava l'affermazione sui media come protesi che amplificano i nostri sensi con il corollario che le protesi tecnologiche "amputano" le parti del corpo e della mente di cui amplificano le funzioni. E così ci ritroviamo ad utilizzare i media digitali senza soffermarci troppo sulle mutazioni sensoriali e cognitive che si stanno producendo, esternalizzando al di fuori del nostro corpo fisico funzioni crescenti: oggi ci apprestiamo a trasferire a software, siti Internet, algoritmi, parte della nostra stessa identità.

Con l'affievolirsi dei confini tra mondo online e mondo offline, in una modalità "always on" favorita dalla rapida diffusione di dispositivi mobili evoluti, la progressiva ibridazione delle dinamiche sociali nei due ambienti è destinata ad aggredire più livelli. Da una parte, tramonta definitivamente il mito dell'anonimato online, della possibilità e della pratica di affidare ad avatar e alter ego digitali un pezzo della nostra personalità, senza che questo vada ad incidere sulla nostra immagine "reale". Dall'altra, la nostra "identità digitale" esce dagli ambienti virtuali e colonizza il mondo "reale". Siamo costantemente tracciati tramite il numero IP dei dispositivi che utilizziamo, il numero di cellulare, le coordinate gps che rilasciamo e tutto lo sciame di tracce digitali che disseminiamo nella nostra quotidianità. Reale e virtuale tendono a coincidere sempre più e in maniera sempre più stringente.

Nella società dei flussi, anche l'identità assume caratteristiche processuali e non può assolutamente essere considerata come uno stato raggiunto o un insieme di caratteristiche dato una volta per tutte. Un'identità costruita, in continuo cambiamento ma in cui è essenziale il governo delle risorse che la vanno a costituire. Una vetrina del proprio sé (Codeluppi 2007) che si integra col nostro corpo nel comunicare al mondo ciò che siamo. Da questo punto di vista, anche le nostre relazioni sociali sono un attributo necessario dell'identità.

A questo punto, le implicazioni problematiche che si aprono (a livello sociale, giuridico, tecnologico, commerciale e politico) sono numerosissime. Basti pensare all'enorme quantità di informazioni personali desunte dalle nostre interazioni con le reti sociali, con i motori di ricerca e i siti di commercio elettronico, così come ai contenuti che ci riguardano generati da altre persone utilizzando potenzialmente una miriade di strumenti e di modalità differenti (pagine Web, tweets, commenti, tag di foto, bottone "mi piace", ecc.). Nel giro di pochi anni, siamo passati da una situazione in cui su Internet "nobody knows you're a dog" (1993) a quella odierna dove "everybody knows you're a dog", con la conseguente esplosione del mercato pubblicitario online.

Occorre tuttavia sottolineare con forza che la natura del problema va ben oltre il tema della privacy per aggredire la questione della proprietà, del possesso e dell'utilizzabilità o meno (e in che contesto) delle informazioni "di contorno" rispetto ai dati definiti come strettamente personali. L'eterna memoria della rete, unita alla globalizzazione dell'utenza, fanno emergere nuove problematiche legate alla

rappresentazione della nostra persona sul Web rispetto alle consolidate abitudini del mondo offline. La nostra immagine digitale, o meglio le innumerevoli immagini ricreate da molteplici soggetti in rete, costituiscono un'impronta del nostro essere accessibile da una quantità di persone molto più ampia. È per questo motivo che negli ultimi anni la cosiddetta *Web reputation* ha assunto un significato sempre più importante e delicato. La reputazione online rientra nell'ambito dei diritti sulla tutela dei dati personali, ribaltando il concetto primordiale di privacy del 1890 "*the right to be let alone*" nel più moderno diritto di decidere come partecipare alla vita pubblica, spesso definito come diritto all'autodeterminazione informativa.
Il nuovo paradigma di comunicazione del Web 2.0 e il proliferare di reti sociali ci pongono davanti alla questione di cosa condividere e con chi. Il vero problema consiste nel non essere in grado di gestire non solo le informazioni che abbiamo immesso in rete noi stessi (per le quali abbiamo una sorta di responsabilità), ma soprattutto quelle che altri hanno pubblicato sul nostro conto. Il processo di pubblicazione online di informazioni, foto, video ecc. è pressoché irreversibile. In questo senso, i più giovani mostrano scarsa consapevolezza dei rischi associati alla gestione di informazioni che li riguardano e siti come http://www.weknowwhatyouredoing.com lo mettono drasticamente in evidenza. D'altronde non è nemmeno auspicabile un mondo in cui, per paura che gli errori del passato siano eternamente visibili e accessibili a tutti, si tenda a limitare la propria libertà di espressione e di comportamento. La gestione della propria reputazione online risponde alle sfide poste da questo difficile equilibrio tra diritto alla riservatezza e libertà di comunicare e include la possibilità di avere il controllo attivo sulle informazioni online che ci riguardano.
Negli ultimi mesi, si è acceso il dibattito in Europa circa l'istituzione di un apposito diritto relativo alla cancellazione di dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o trattati e quando l'utente abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano, ovvero il diritto all'oblio. Questo concetto, introdotto dall'art. 17 del nuovo regolamento generale europeo sulla protezione dei dati personali – attualmente in fase di discussione al Parlamento Europeo – viene rafforzato nell'ambiente online nel quale si pone l'obbligo, per il responsabile del trattamento che ha pubblicato dati personali, di informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. In questo possibile scenario, si contrappongono un principio etico e la complessità della sua implementazione tecnica, a partire dalla realizzazione di quanto previsto nel nuovo regolamento: gli operatori potrebbero infatti essere indotti a rafforzare le forme di tracciamento di foto e video, accrescendo ulteriormente il problema del tracciamento, piuttosto che risolvere quello dell'oblio.
D'altronde già 400 anni orsono Francis Bacon aveva espresso il concetto che "*ipsa scientia potestas est*" (la conoscenza stessa è potere). Ora la questione è che mentre perdiamo parte del controllo sulle informazioni personali, qualche altro soggetto acquisisce potere dalla nostra perdita, basti pensare a Google e Facebook. Tali colossi spesso utilizzano le informazioni che abbiamo fornito in modo più o meno consapevole e tendono a mantenere l'utente chiuso nei propri sistemi senza possibilità di esportare le proprie informazioni su piattaforme di servizi similari (*customer lock-in*). Anche questo tema viene affrontato nel nuovo regolamento europeo sulla protezione dei dati personali in cui si sancisce il diritto alla

portabilità dei dati e l'obbligo da parte del fornitore di servizi di fornire all'interessato copia dei dati trattati in un formato elettronico e strutturato che sia di uso comune e gli consenta di farne ulteriore utilizzo.
Sebbene secondo il co-fondatore di Facebook, Mark Zuckerberg, l'era della privacy sia finita, le recenti statistiche mostrano come gli utenti abbiano molto a cuore la protezione del proprio ambito personale, sia nel mondo reale che in quello virtuale. Non ci resta pertanto che attendere che vengano riconosciuti alcuni diritti fondamentali dell'uomo anche nello spazio in cui passiamo sempre più tempo: quello digitale.

Scenario internazionale

A livello internazionale si sta affermando una visione comune a molti Paesi che pone la gestione dell'identità digitale come obiettivo primario oltre che per lo sviluppo di servizi di e-government, anche per l'innovazione dei servizi online (pubblici e privati) e l'aumento della sicurezza informatica al fine di favorire la crescita dell'economia su Internet (OECD 2011). Molti Paesi hanno preferito adattare o estendere le procedure di identificazione tradizionali piuttosto che re-ingegnerizzare completamente i processi. In generale, le politiche di registrazione[1] dei cittadini possono essere basate su approcci centralizzati o de-centralizzati. Nel primo caso, il processo di registrazione avviene tramite un registro della popolazione e solitamente si assegna un unico identificativo a ogni cittadino, mentre nel secondo caso ogni organizzazione è autonoma rispetto al proprio modello di registrazione. Nel seguito vengono analizzati sinteticamente alcuni esempi europei e nordamericani per comprendere le differenze tra i vari approcci. La situazione italiana viene descritta in modo più dettagliato nel riquadro fornito separatamente.
La **Germania** sta migrando dalla carta d'identità cartacea a quella elettronica fornendo ai cittadini un token universale per l'autenticazione per le comunicazioni di e-gov e e-business. Il portale dei cittadini è certificato e fornisce email sicure, servizi per la verifica dell'identità e cassette di sicurezza per documenti. Sono stati definiti i dettami tecnici per l'interoperabilità e l'utilizzo sicuro dell'identità digitale per le piattaforme amministrative. L'utilizzo di un unico identificativo numerico per i cittadini non è consentito dalla Costituzione, pertanto gli utenti vengono identificati attraverso un set di attributi e i numeri identificativi sono specifici del settore di appartenenza. La Germania adotta una strategia centralizzata che non poggia su un unico identificatore nazionale.
Nel giugno del 2010 gli **USA** hanno redatto la bozza di "*National Strategy for Trusted Identities in Cyberspace*" che promuove l'utilizzo di sistemi di identificazione per l'accesso ai servizi online che siano sicuri, efficienti, facili da usare e interoperabili. L'obiettivo è quello di aumentare fiducia, privacy, offerta e innovazione. Viene introdotto il concetto di un ecosistema di fornitori di servizi di identificazione interoperabili e parti coinvolte in cui gli individui possano scegliere se utilizzare credenziali singole o differenti per i vari tipi di operazioni online. L'approccio americano si basa su un processo di registrazione de-centralizzato e adotta un modello d'identità federato.
Il **Canada** ha sviluppato la cosiddetta "*Pan-Canadian strategy*" che mira a offrire servizi governativi multi-canale, utilizzando politiche di registrazione de-centralizzate e adottando un modello di fiducia federato in cui i soggetti coinvolti mantengono il massimo livello di autonomia. Molte particolarità e sfide

[1] Il processo che collega legalmente l'individuo alla propria identità digitale.

LA SITUAZIONE ITALIANA

L'Italia sta lentamente migrando dalla carta d'identità cartacea alla carta nazionale dei servizi (CNS) e alla carta d'identità elettronica (CIE), che mirano a soddisfare i requisiti dei servizi di e-gov. Le carte hanno caratteristiche simili e compatibili e permettono l'autenticazione ai servizi di e-gov e (opzionalmente) la firma digitale, anche se la carta nazionale dei servizi non include caratteristiche di sicurezza fisica per verificare l'identità offline. In base al Codice dell'Amministrazione Digitale (CAD), le nuove carte elettroniche costituiscono strumenti per l'accesso ai servizi erogati online dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica. Inoltre, le disposizioni relative all'accesso ai documenti informatici e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici e agli organismi di diritto pubblico. L'Italia adotta una politica di registrazione centralizzata dove i soggetti che effettuano la registrazione (gestiti dai Comuni) sono centralizzati a livello nazionale e il codice fiscale è un identificativo unico per tutti i registri pubblici.

La possibilità di accedere ai servizi della pubblica amministrazione mediante la carta nazionale dei servizi e la carta d'identità elettronica esiste da anni e costituisce una modalità affidabile, ma di utilizzo non sempre semplice, per verificare le identità degli utenti (ad esempio è necessaria la disponibilità di un lettore di carte elettroniche). Nell'ambito del quadro normativo italiano, una novità importante è intervenuta recentemente nella fase di conversione in legge del DL 21 giugno 2013 n. 69, meglio noto come "Decreto del fare". In questa fase, che ha portato all'emanazione della legge del 9 agosto 2013 n. 98, tra le varie modifiche al Codice dell'Amministrazione Digitale (CAD), è stata aggiunta quella che prevede l'istituzione, a cura dell'Agenzia per l'Italia digitale, del cosiddetto Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID). Il sistema SPID ha lo scopo di agevolare l'accesso, anche in mobilità, ai servizi in rete da parte di cittadini e imprese e prevede che soggetti pubblici e privati, accreditati dall'Agenzia per l'Italia digitale, gestiscano "i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati" (art. 64 comma 2 ter del CAD). Con un apposito DPCM, per il quale sarà anche sentito il Garante per la protezione dei dati personali, verranno definite le caratteristiche del sistema SPID, nonché i tempi e le modalità di adozione del sistema stesso da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete. Tra le caratteristiche che il DPCM dovrà specificare vi saranno in particolare:

a) il modello architetturale e organizzativo del sistema;

b) le modalità e i requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) gli standard tecnologici e le soluzioni tecniche e organizzative da adottare;

d) le modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) le modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

di questo sistema derivano dall'approccio de-centralizzato della registrazione, basti pensare all'interoperabilità delle credenziali intra e inter sistemi pubblici e privati. Ogni istituto è responsabile per il tipo di credenziali, la scelta dei dati personali identificati, il livello di sicurezza e l'informativa agli utenti circa benefici e rischi. Le criticità riguardano le incongruenze tra le varie giurisdizioni, quali ad esempio requisiti legali, lingua e accessibilità. ■

BIBLIOGRAFIA

"OECD, *National Strategies and Policies for Digital Identity Management in OECD Countries*, 31 marzo 2011.
Bolter J.D. e Grusin R., 2002, *Remediation*, Milano, Guerini e Associati.
Codeluppi V., 2007, *La vetrinizzazione sociale*, Torino, Bollati Boringhieri.
McLuhan M., 1964, *Understanding Media: The Extensions of Man*, NY, McGraw Hill.
Rodotà S., 2005, (a c. di P. Conti), *Intervista su privacy e libertà*, Roma-Bari, Laterza.
Tursi A., 2011, *Politica 2.0*, Milano, Mimesis.