Come verificare digitalmente l'identità umana

Il caso delle votazioni

Quanto è realmente importante l'identità individuale nell'essere umano? Da irrilevante a fondamentale ogni risposta è possibile, ma solo definendo il contesto possiamo ottenere una risposta. Nella preistoria, probabilmente non esisteva un'identità personale ma solo un identità dicotomica di gruppo. I soggetti appartenevano ad un gruppo utilitaristico che poteva essere di amici o nemici, maschi o femmine, forti o deboli e così via. Invece oggi l'identità personale è indispensabile per la convivenza delle persone nella società. Ogni individuo ha una sua storia registrata e delle identità per aiutare a favorire le relazioni con gli altri o per accedere a dei servizi.

Evoluzione tecnologica e nuove abitudini sociali hanno esasperato questa esigenza di identificare con crescente precisione la persona. Per condurre un automobile è necessaria una patente di guida nominale, per visitare uno stato estero è necessario il passaporto, per una visita medica è necessario il codice sanitario (o equivalente), per esercitare il diritto di voto è necessaria la carta d'identità (o equivalente). Di contro, questo eccesso di informazioni usate per l'identificazione si contrappone al necessario rispetto dei diritti e libertà fondamentali degli individui alla privacy, ed in particolare, al loro diritto alla protezione dei propri dati personali. La difficoltà sta nel determinare il giusto bilanciamento tra l'efficacia dell'identificazione ed il diritto alla privacy della persona.

Definizione dell'identità umana

L'identità umana è l'insieme delle caratteristiche che rendono unico un individuo nella società (quando si fa riferimento ad un singolo individuo, non alla specie umana nel suo insieme). Nel contesto sociale è un metodo per identificare una persona rispetto alle altre. In termini informatici possiamo definirla come un oggetto avente un codice univoco, internamente ad uno spazio di definizione, associato a vari attributi ed a metodi di trattamento. Definire in astratto l'identità è facile, ma nella pratica, la difficoltà deriva dai diversi modi di scegliere o trattare le caratteristiche individuali per identificare il soggetto. Talvolta, in aggiunta alle informazioni strettamente necessarie al riconoscimento dell'identità, vengono richieste ulteriori classi di informazioni quali, ad esempio, indirizzo, genere, età, foto. Alcune di queste, non sono propriamente finalizzate al riconoscimento ma al solo tracciamento di profili comportamentali. Inoltre, questi dati nel tempo

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

È lead auditor e consulente senior su tematiche di risk management, cybersecurity e privacy. È stato responsabile del monitoraggio dei rischi presso un'azienda multinazionale del settore automotive per oltre sette anni. In precedenza, è stato responsabile della gestione dei servizi e delle risorse ICT nell'area Asia-Pacific (Cina, Giappone e Malesia) e, prima ancora, è stato responsabile della sicurezza delle informazioni a livello mondo per più di sette anni. Per quanto attiene al monitoraggio interno del rischio, ha sviluppato una metodologia originale integrando tra loro, analisi del rischio operativo, valutazione del livello di maturità dei controlli e risk-based Internal Audit. I processi aziendali sono paragonati a servizi cooperanti basati sui principi guida del framework ITIL 4 e del Manifesto Agile. Inoltre, ha progettato uno strumento di cyber monitoring e un sistema integrato per monitoraggio del rischio, modello di maturità e audit interno. Sbriz è stato anche consulente per sistemi di business intelligence per parecchi anni. Può essere contattato su LinkedIn *https://www.linkedin.com/in/luigisbriz* oppure tramite *http://sbriz.tel.*

potrebbero avere necessità di cambiamento, o per aggiornamento delle caratteristiche personali o per cessazione del servizio o per errata registrazione o per qualunque altra esigenza dell'interessato.

Il metodo di identificazione impiegato deve permettere di individuare (autenticare) un soggetto in modo soddisfacente, per conseguentemente riconoscergli il diritto (autorizzare) a compiere determinate azioni o vietarne altre ancora. A volte non serve la certezza di aver identificato correttamente l'individuo che richiede un servizio, ma è sufficiente ottenere una adeguata garanzia di un uso lecito del metodo di identificazione assegnato per l'accesso. Ossia, se le credenziali presentate sono ritenute autentiche o il dispositivo è riconosciuto, allora l'operazione è comunque autorizzata. Per esempio, se il prelievo di contante da un ATM viene fatto da un soggetto diverso dal titolare del conto bancario, ma in possesso delle giuste credenziali, l'operazione è ritenuta lecita perché l'identificazione è fatto sulla coppia dispositivo fisico e password. Il titolare del conto è consapevole delle conseguenze di perdita dispositivo o divulgazione password e si assume la responsabilità della diligente custodia.

La costruzione di una identità realistica da utilizzarsi in rete, non può limitarsi ad una mera opzione tecnologica ma deve includere una rappresentazione astratta della persona, dei comportamenti e delle caratteristiche distintive dell'individuo. Inoltre, le caratteristiche da considerare devono seguire l'evoluzione della tecnologia e richiedere adeguamenti periodici, se nel tempo si alterano. La ragione primaria di assicurare l'aggiornamento costante del profilo di identità, è per contrastare efficacemente la falsificazione o la sostituzione dell'identità. Pensiamo al deep fake che altera in modo verosimile le forme umane nelle rappresentazioni grafiche del mondo reale, rendendo difficile la verifica di autenticità delle identità presenti.

Non esiste una singola soluzione per la gestione del riconoscimento dell'identità in rete. Il metodo proposto distinguerà tra due tipi di registrazione dell'identità, per differenti complessità e caratteristiche:

1. Registrazione di un identità reale, sicura, certificata, per essere di riferimento per altre identità. Per garantire queste proprietà, sarà richiesta la certificazione di un'autorità, e quindi non sarà possibile ricorrere ad una procedura interamente online. È necessario il riconoscimento fisico per dare valore alla registrazione stessa ed attivare la conseguente identità online certificata.
2. Un'identità che viene facilmente utilizzata per le attività quotidiane, e la sua emissione deve essere necessariamente agevole, veloce ed ovviamente sicura. Sarà usata esclusivamente online e certificata tramite il primo tipo di identità.

Prima di esporre lo schema di gestione delle identità in rete, analizziamo le differenze di una serie di registrazioni di identità usate nella vita reale, per capire quante diverse situazioni e soluzioni sono state adottate per uno stesso tipo di problema: quello di riconoscere l'identità di una persona.

Contesti dove viene richiesta l'identità

Nelle situazioni della vita reale dove è necessario dimostrare la propria identità, l'identificazione viene gestita in prevalenza, o con documenti fisici emessi da enti governativi o con credenziali elettroniche emesse dal sistema dell'organizzazione che autentica la validità delle credenziali stesse. Alcuni degli esempi più comuni sono illustrati nella **figura 1**.

Esistono innumerevoli altre situazioni in cui viene creato un profilo utente e vengono emesse le credenziali di autenticazione, sebbene ogni circostanza possa avere requisiti diversi per l'identificazione. Vale anche la pena notare che non tutte le richieste di dati personali sono regolamentate dal principio del need-to-know. Questo è un principio di base della sicurezza delle informazioni, che significa, ridurre all'indispensabile le informazioni trattate, e la sua violazione può compromettere seriamente la privacy.

Registrazioni e profili personali

Una prima preoccupazione emerge dall'elevato numero di registrazioni d'identità, il ripetuto conferimento di dati personali ai fornitori dei servizi, crea a una sorta di abitudine e questo significa un calo di attenzione. Non solo il numero di registrazioni espone a rischio i nostri dati personali, ma anche a volte la carenza di spiegazioni esaustive sulla necessità di fornire taluni dati e sul loro trattamento. Nel caso di cessazione, dovuta a specifica richiesta o mancato rinnovo, del servizio per il quale erano stati forniti i dati personali, non sempre questi vengono prontamente cancellati secondo i termini previsti (contrattuali e di legge), esponendoli a rischio di uso non autorizzato o illegale (ad es., furto d'identità).

La contromisura, al problema del numero di registrazioni ed alla quantità di dati personali immessi, è il ricorso ad un fiduciario che abbia la custodia dei nostri dati personali ed abbia la facoltà di

FIGURA 1

Tipologie di identità utilizzate nel quotidiano

Documento o processo	Identità	Caratteristiche
Passaporto	Digitale ma statica (rinnovo dopo anni)	Possiamo ridurlo ad un oggetto composto da due parti: le informazioni dell'identità pubblica del soggetto e quelle di accesso in un altro paese. I dati pubblici sono parzialmente visibili (ad es., dati anagrafici e foto) mentre quelli biometrici della persona e di integrità del documento fisico sono accessibili tramite firma digitale.[a]
Carta d'identità	Digitale ma statica (rinnovo dopo qualche anno)	Dovrebbe essere il documento di riferimento dell'identità di una persona, ma nasce per un uso manuale, e per quanto abbia dei dati in formato digitale (ad es., banda magnetica, chip di sola lettura, olografia), non è strutturato per affrontare il confronto con le tecnologie attuali e la loro evoluzione.
Patente di guida	Digitale ma statica (rinnovo dopo qualche anno)	Come per il passaporto è formata da due tipi di informazioni, uno di identità e l'altro di dati specifici di abilitazione alla guida. Quest'ultimi dati sono l'obiettivo del documento ma solo dopo aver abbinato la corretta identità.
Codice fiscale	Statica, leggibile elettronicamente	Nasce come codice univoco associato ad un individuo per aiutare il tracciamento delle attività con la pubblica amministrazione o gli enti governativi. Non ha obiettivi di autenticazione dell'identità, ma solo di puntatore ai dati della persona. Talvolta è richiesto su qualche sito web per ridurre la duplicazione degli utenti.
Credenziali bancarie	Digitale, dinamica, strong authentication	Oramai prevalentemente digitali, variano in relazione all'evoluzione delle tecnologie di sicurezza ma non autenticano direttamente la persona. Sono piuttosto autoreferenziali, verificano che le credenziali stesse siano realmente quelle assegnate. Separatamente, ogni banca o circuito di pagamento conserva i dati identificativi della persona ed il profilo di rischio.
Carta fedeltà	Statica, leggibile elettronicamente	Anche se nominale, non ha l'obiettivo di riconoscere la persona ma solo di avere un puntatore ai dati d'acquisto del portatore. L'esigenza è quella di identificare il profilo d'acquisto che potrebbe anche essere associato ad un gruppo di persone, tipo una famiglia.
Smartphone	SIM e device ID	La SIM card è un circuito integrato che memorizza il numero di telefono (cioè, l'identità internazionale del cellulare), prima ancora di quella della persona. Non c'è garanzia sulla identità dell'utilizzatore ma l'autenticazione del dispositivo è garantita da una valida regolamentazione internazionale. Similmente le eSIM, versione soft della SIM.[b]
Procedura di voto	Riconoscimento fisico	Generalmente l'identità della persona fisica è autenticata tramite documento d'identità prima di accedere alla cabina elettorale. È il procedimento più sicuro ma richiede ai votanti di accedere fisicamente al seggio elettorali.
	Voto postale	Il voto postale è basato sul principio della doppia busta, quella esterna è per l'identificazione del mittente, quella interna è anonima per la segretezza del voto. Il controllo è di congruenza dei dati di spedizione e di integrità delle buste utilizzate. Il processo di spoglio è lento e non fornisce sufficienti garanzie sulla libera espressione del voto.
	Voto elettronico remoto	Il voto elettronico da remoto (via Internet) usa lo stesso concetto di quello postale. Le buste fisiche sono sostituite da messaggi digitali incapsulati. Quello esterno è firmato digitalmente dal votante, quello interno è anonimo. È una valida risposta tecnologica alla lentezza delle operazioni di spoglio, tuttavia la libera espressione del voto non è verificata ed esiste il rischio di frodi informatiche[c, d].

Sources: a) International Civil Aviation Organization (ICAO), "Public Key Directory: Secure Cryptographic Authentication of Chip-Based Traveler Information," *https://www.icao.int/Security/FAL/PKD/Pages/default.aspx*; b) GSMA, "eSIM," *https://www.gsma.com/esim/*; c) American Association for the Advancement of Science (AAAS), "Internet or Online Voting Remains Insecure," USA, 10 March 2021, *https://www.aaas.org/epi-center/internet-online-voting*; d) e-Estonia, "i-Voting—The Future of Elections?" 6 March 2019, *https://e-estonia.com/i-voting-the-future-of-elections/*

operare in un ecosistema controllato. Un ecosistema fatto di tecnologie, protocolli ed operatori di provata fiducia[1, 2]. L'unico vero garante dell'identità reale e completa di una persona è l'ente governativo che gestisce la nostra identità legale, quello che rilascia la carta d'identità fisica. Questo non vuol dire che deve esistere un unico enorme database fisico con tutte le classi dei nostri dati personali, ad esempio, anagrafici, sanitari, giudiziari, scolastici, lavorativi e così via. Solamente che deve esistere un unico sistema di controllo accesso ai database governativi.

In pratica, è come avere accesso ad un enorme database virtuale dei nostri dati originali, gestito da un custode statale (ente governativo) e quindi di fiducia, che ha l'autorità di regolamentare le operazioni di registrazione dell'identità digitale legale dei cittadini, di rilasciare un certificato digitale personale (**figura 2**) e di garantire la conferma della nostra identità legale ai soggetti che lo richiedono per un legittimo interesse.

Schema di una soluzione di identità via Internet (I-Identity)

Tecnicamente, per riconoscere con sicurezza un utente su Internet con un meccanismo che dia garanzie di affidabilità e praticità è necessario ricorrere a sistemi di identità digitale federata. Devono essere costruiti su standard di autenticazione aperti, ad esempio OpenID Connect 1.0 (OIDC)[3] che adotta il protocollo di autorizzazione OAuth 2.0 basato sullo scambio di token[4], ma non deve mancare la possibilità di aggiungere delle opportune estensioni, quali la categorizzazione degli identity provider. Supponiamo che una persona (cittadino) richieda tramite Internet la creazione di un profilo utente per accedere ad un nuovo servizio (service provider). In alternativa al classico inserimento di dati personali con eventuale invio della copia della carta d'identità, ripetuto su ogni nuovo sito web, è più efficace un meccanismo online interamente basato su certificati digitali emessi da un autorità di certificazione (identity provider), che garantisce l'integrità delle informazioni ricevute da un'autorità pubblica (custode statale). La persona deve possedere un certificato digitale personale (P), sia per gestire i rapporti con la pubblica amministrazione, che per ottenere uno o più certificati digitali comuni (C) per le attività quotidiane. Il certificato digitale è un mix di informazioni sulla persona, sul dispositivo e sull'organizzazione di fiducia che lo emette e lo firma tramite crittografia.

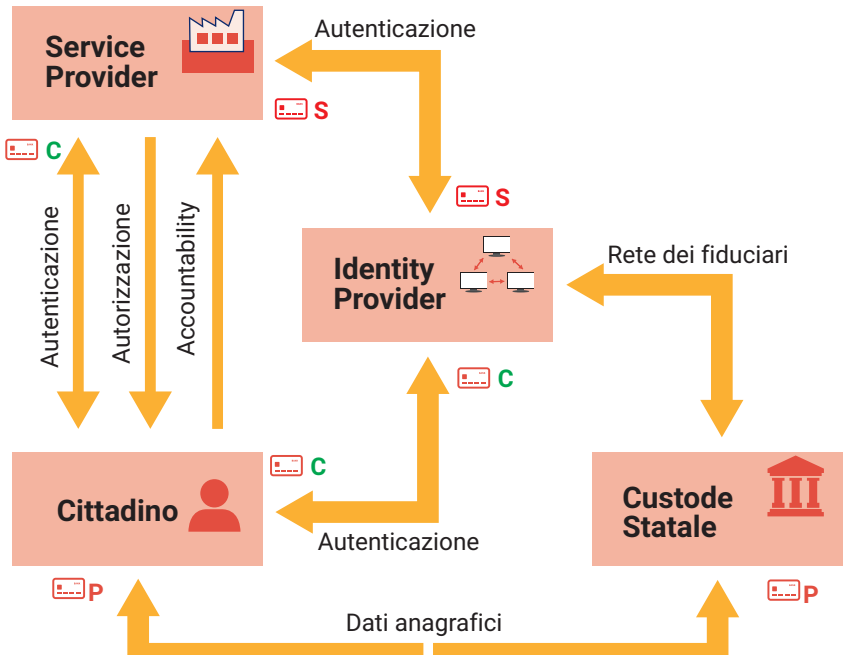
Il certificato personale (P) è rilasciato da un autorità pubblica (custode statale) a seguito di un riconoscimento fisico presso un'autorità locale pertinente alla residenza del cittadino. Il custode statale va pensato come una infrastruttura ad albero, sulla cima ci sono i dati mentre sulle radici gli enti governativi, che provvede al governo dei certificati privati, inclusa anche l'autorizzazione di accesso alle categorie dei dati personali sulla base del profilo autorizzativo del richiedente. Ad esempio, per un controllo stradale, saranno resi disponibili alla polizia tutti i dati personali del conducente relativi alla dimostrazione della capacità di guidare un veicolo. In generale, tutti i dati necessari ai servizi pubblici, sociali e civili, saranno nella disponibilità dei rispettivi organi di controllo pubblici. Una blockchain centralizzata registrerà tutte le query di identificazione per eventuali analisi forensi, mentre strumenti di analisi del traffico di rete, lo verificheranno abbinando richiedente, classe autorizzativa, dispositivo, tipologia dato, classificazione dato, per creare allarmi e segnalare eccessi o abusi di trattamento dati.

Il certificato comune (C) è rilasciato dal proprio garante dell'identità pubblica (identity provider) a seguito di un riconoscimento online con l'autorità pubblica (custode statale). Il custode statale, in quanto garante dell'identità di livello più elevato, interagisce con i fornitori di identità pubblica su una apposita overlay network. Restituisce una classe di dati personali a seguito dell'autenticazione del certificato privato. Questo consente al fornitore di identità di creare il nome utente ed il certificato da usare in pubblico ed inviarlo al richiedente. È verosimile che questa operazione richieda un abbonamento a pagamento.

Con il nome utente pubblico ed il certificato comune, la persona può aprire un proprio profilo presso il fornitore del servizio che vuole attivare. Nel modulo di registrazione viene inserito il nome utente, con suffisso il nome dominio del fornitore di identità, ed in alternativa alla password, viene scelto l'invio

FIGURA 2

Schema del riconoscimento dell'identità su Internet



del certificato comune con la selezione delle classe di dati personali da comunicare automaticamente. Esempi di classi dati possono essere nome, indirizzo, nascita, genere, e così via. Le classi disponibili sono ristrette a quelle possedute dal fornitore di identità, che non dovrebbero eccedere quelle presenti nella carta di identità fisica. Per inviare più dati, è necessario definire un meccanismo più ampio, regolamentato da uno standard internazionale creato per questa circostanza, coinvolgendo anche il custode statale.

In automatico, il service provider invia al proprio identity provider, il certificato del richiedente (C) ed il proprio certificato (S). Questa operazione permette la validazione dell'identità di entrambi, il richiedente ed il fornitore del servizio. Quindi, sempre in automatico, il richiedente il servizio, viene informato della registrazione delle attività per dimostrare la legittimità delle azioni compiute. A questo punto, il sistema del service provider concede i privilegi ed i permessi di accesso ai dati.

Questo schema di identificazione è molto sicuro in quanto basato su più fattori: il riconoscimento del dispositivo (incluso nel certificato), l'indirizzo di rete del richiedente (incluso nel package di autenticazione), la capacità di contattare l'emittente del certificato (verifica di integrità) e la robustezza delle chiavi crittografiche (crittografia sia del canale di comunicazione che dei dati). La forza del meccanismo è legata alla possibilità di compiere immediati controlli sui fattori citati e con una scelta di tecnologia adeguata a ciascuno di essi. È una specie di difesa in profondità, verifica dell'origine della richiesta (dispositivo, indirizzo), dell'identità dell'emettitore (certificato), della correttezza del destinatario (consenso), dell'integrità dei messaggi (crittografia). Lo sforzo è focalizzato al contrasto delle false identità.

Lo schema di identificazione può essere generalizzato rimuovendo il vincolo dello stesso identity provider per richiedente e service provider. Entrambi possono autenticarsi su un proprio identity provider e quasi nulla cambierà, tranne uno scambio di certificati tra i due identity provider per accertarsi della validità del certificato emesso dall'altro provider.

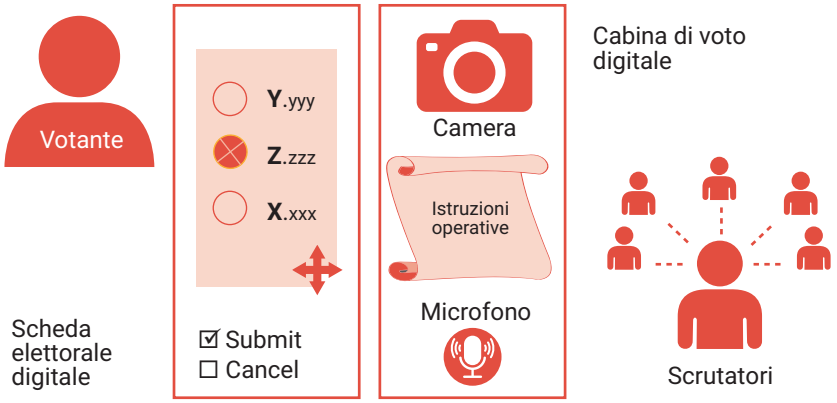
Schema di una soluzione di voto via Internet (I-Voting)

Un'altra possibile applicazione legata alla certificazione dell'identità della persona fisica è il voto sicuro via Internet. In generale, la votazione elettronica (e-voting) presenta diversi metodi finalizzati a semplificare l'espressione del voto ed il celere conteggio delle preferenze attraverso tecnologie elettroniche e/o informatiche. Tra questi, si vuole portare l'attenzione sui metodi che si attuano per mezzo di Internet (I-voting), con il fine di proporre un processo che sappia coniugare il mezzo più diffuso al mondo nell'ambito delle comunicazioni, Internet, con i requisiti basilari di una votazione pubblica. Quattro sono i requisiti primari del voto: il diritto al voto, la libertà di espressione del voto, l'identità certa del votante e la segretezza del voto. Il diritto al voto richiede che non ci siano impedimenti ad esprimere il voto stesso. La difficoltà ad accedere al sito, ove è installata la cabina elettorale, può fare la differenza alla partecipazione al voto. Sviluppare un'applicazione per il voto tramite Internet (I-voting), basata sull'identità digitale certificata da una rete di fiduciari dell'identità, non richiede un particolare sforzo tecnico, ma attualmente non è abbastanza. Deve essere abbinata a procedure di controllo remote gestite da operatori.

I componenti principali sono tutti disponibili, vanno solo messi assieme. Ci sono protocolli per gestire l'autenticazione e ci sono anche programmi di intelligenza artificiale (IA) per riconoscere una persona ripresa da una webcam. Però, il requisito legato alla libertà di espressione del voto richiede comunque un giudizio umano (in attesa di ulteriori evoluzioni dell'IA). Il software dovrebbe essere di tipo open source ed il controllo umano remoto garantisce gli aspetti legati alla libertà di voto. Un'applicazione di voto scaricabile sullo smartphone personale potrebbe avere le seguenti caratteristiche (**figura 3**) per salvaguardare i criteri richiesti ad un sicuro ed efficace processo di voto.

FIGURA 3

Schema di voto tramite applicazione su smartphone



Il votante, tramite l'applicazione sullo smartphone, su connessione crittografata, è autenticato con il certificato digitale personale emesso dal custode statale. Il software di riconoscimento facciale, attingendo ai dati personali del custode, valuta l'identità fisica ed agisce come primo filtro per consentire l'accesso all'ufficio elettorale virtuale. Questo è un call-center di persone selezionate con gli stessi criteri di un seggio elettorale fisico. Ogni operatore potrà interagire con più votanti contemporaneamente ed ha almeno un supervisore che monitora le sue attività. Un breve insieme di istruzioni testuali, informerà il votante della necessità di abilitare l'operatore a prendere il controllo del dispositivo, in particolare, camera e microfono ma senza poter vedere i contenuti della scheda di voto virtuale. Se il votante acconsente, dopo una ricognizione ambientale con camera e microfono, la votazione ha inizio.

Le analogie con la votazione fisica sono ovviamente molte. Il votante è riconosciuto prima di accedere al voto. L'ufficio elettorale virtuale, tramite il controllo ambientale ottenuto operando dal dispositivo, garantisce che il votante sia libero di agire senza condizionamenti di altri (da solo come all'interno della cabina elettorale). All'operatore remoto è sempr inibita la visione delle operazioni sullo schermo del votante, garantendo la segretezza. Tra l'altro, le scelte di voto della scheda elettorale possono essere mescolate casualmente per impedire di dedurre, dall'osservazione dei movimenti della mano (se inquadrata dalla camera), la selezione fatta. L'operatore può bloccare l'operazione di voto in caso di infrazione delle regole elettorali. Dopo aver completato le selezioni e confermato il voto, lo smartphone si sblocca ed il votante lo può utilizzare nuovamente in piena libertà.

Opzioni per il seggio elettorale

Anche se è resa disponibile un'applicazione su smartphone, l'opzione del voto di persona sarà comunque necessaria per chiunque abbia ostacoli come motivi di costo, o di familiarità nell'uso dello smartphone, o di fiducia nella soluzione, o semplicemente perché una soluzione di backup è necessaria. Per allestire una cabina elettorale elettronica, si possono utilizzare desktop, laptop o tablet con una versione del software che, se presenti, camera, microfono e tastiera saranno disabilitati ma mouse (o touchscreen) abilitato. Le disabilitazioni servono perché il controllo è fatto fisicamente dal personale elettorale, mentre il modulo software della manifestazione di voto resta invariato. Il software deve essere su dispositivo rimovibile autoavviante, gestito direttamente dalle autorità, con un certificato digitale identificativo della cabina elettorale, per poter utilizzare qualsiasi computer senza modificare la sua configurazione. L'operazione di voto viene attivata dal personale elettorale inviando alla cabina elettorale un messaggio di abilitazione (es. via Bluetooth, via Wi-Fi) composto dal codice identificativo della cabina elettorale, il codice fiscale del votante ed il certificato del funzionario elettorale. In fase di costituzione del seggio elettorale, vengono distribuiti i certificati digitali necessari ed abilitati i dispositivi utilizzati dal personale elettorale.

Per agevolare persone impossibilitate ad accedere al seggio elettorale, è possibile allestire una cabina elettorale mobile, utilizzando un tablet o un laptop e seguendo la procedura di costituzione di un seggio elettorale. Il personale elettorale dedicato dovrebbe, nell'ordine, raggiungere e riconoscere il votante, abilitare il dispositivo del voto, consegnarlo alla persona (o al suo tutore legale) e assicurare la riservatezza del voto. Ultima considerazione, presso i seggi elettorali, è utile approntare una cabina di simulazione dell'operazione di voto, per risolvere situazioni di mancanza di alfabetizzazione digitale.

Conclusioni

Per gestire efficacemente l'identità di una persona in rete, la soluzione deve essere di semplice utilizzo, sicura per evitare contraffazioni, inoltre, non sempre può essere affidata esclusivamente alla tecnologia, a volte richiede un aiuto umano come nel caso descritto nella soluzione proposta di I-voting. Nello stesso tempo, deve garantire un lecito livello di anonimato, per evitare eccessivi trattamenti del dato personale, per limitare l'impatto del furto di identità e per rendere più efficace il rispetto delle normative sulla privacy. Come per i documenti reali, l'origine delle informazioni personali è sotto la tutela di organismi governativi, che significa avere un arbitro per far valere le giuste ragioni in caso di controversie, e analogamente, tutelare la controparte che eroga servizi.

Il meccanismo proposto di I-identity ricerca un equilibrio tra la complessità delle componenti tecnologiche necessarie, il processo di gestione degli identity provider ed la facilità d'uso per l'utente. Il ricorso ad un ente governativo, come custode dei dati originali dell'identità della persona, non è nulla di nuovo. Non è minimamente una perdita delle proprie libertà individuali perché è un'analogia di

ciò che già esiste ed è alla base dell'ordinamento della vita sociale. La tecnologia è semplicemente un ottimo mezzo per rendere molto più efficiente questo processo. L'uso di documenti digitali è una soluzione sostenibile in termini di risorse, praticità ed è perfettamente ritagliata all'uso in rete. Per ragioni di efficienza e praticità nello svolgimento di attività di rete quotidiane che non richiedono la certezza dell'identità, ad esempio richiedere un film, è possibile utilizzare identità semplificate (gestite dai fornitori di identità) in aggiunta all'identità personale legale (gestita dal custode), che è univoca, reale e ufficiale. La gestione di questo processo non richiede un sistema enorme e complesso, ma una rete di garanti dell'identità in grado di fornire flessibilità ai picchi di domanda, assicurare la resilienza del servizio e garantire la sicurezza.

Questo ecosistema di infrastrutture tecnologiche, protocolli ed operatori, garantendo in modo affidabile e pratico il riconoscimento della persona, permette di ottenere una elevata sicurezza in rete, costi ammissibili e minori contestazioni. Tali benefici possono essere osservati nel processo elettorale. In generale, l'affidabilità e sicurezza del I-identity possono anche essere una spinta a creare nuovi servizi di e-government, per includere i cittadini in un sistema tecnologico più ecosostenibile ed efficiente.

Riferimenti

1. Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 1", *ISACA® Journal*, vol. 2, 2022, https://www.isaca.org/resources/isaca-journal
2. Sbriz, L.; "A Symmetrical Framework for the Exchange of Identity Credentials Based on the Trust Paradigm, Part 2", *ISACA Journal,* vol. 2, 2022, https://www.isaca.org/resources/isaca-journal
3. OpenID, Specifications, *https://openid.net/developers/specs/*
4. OAuth, OAuth 2.0, *https://oauth.net/2/*