DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Il progetto di IT-Wallet

28 Marzo 2024

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners
Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners
Gaia Leoncini, Ristuccia Tufarelli & Partners

DB non solo diritto bancario

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners

Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners

Gaia Leoncini, Ristuccia Tufarelli & Partners

Luca Tufarelli

L'avvocato Luca Tufarelli, Partner e socio fondatore dellotudio Ristuccia Tufarelli & Partners, ha conoscenze specifiche nei campi del diritto civile, commerciale, amministrativo e del diritto dell'informatica dove assiste sia soggetti privati che pubblici. Ha contribuito alla realizzazione di progetti speciali nei settori delle tecnologie innovative, delle telecomunicazioni, della informatizzazione della PA e del commercio elettronico occupandosi anche degli aspetti consumeristici e di compliance regolamentare (privacy, tutela del mercato e vigilanza delle comunicazioni).

Studio associato

Ristuccia Tufarelli & Partners

1. Il contesto di riferimento: il progetto di Digital Identity Wallet

L'attuale contesto socio economico, caratterizzato dalla digitalizzazione di gran parte delle attività economiche e dei rapporti di interazione e servizio con i consumatori ed i cittadini, ha subito un'accelerazione grazie alla crisi pandemica. Nel frattempo questa accelerazione ha aumentato il numero delle persone che utilizzano sistemi digitali e anche la propensione di tutti gli operatori del mercato e dei servizi, compresi quelli pubblici, a digitalizzare i processi. C'è stata quindi una crescita esponenziale della domanda di mezzi per identificarsi e autenticarsi online, nonché per scambiare digitalmente informazioni in maniera sicura.

La disciplina dell'identificazione elettronica è contenuta nel Regolamento (UE) n. 910/2014, il c.d. regolamento eIDAS ("*electronic IDentification Authentication and Signature*"), il quale prevede che l'identità digitale ("eID") di uno Stato dell'Unione possa essere utilizzata per accedere ai servizi online dell'amministrazione pubblica di tutti gli Stati europei in forza di un reciproco riconoscimento dei mezzi di identificazione elettronica.

L'obiettivo primario del Regolamento eIDAS è quello di garantire la piena interoperabilità tra gli Stati membri (i) degli strumenti di firma elettronica certificata (in Italia firma digitale), (ii) dell'identificazione web dei cittadini (in Italia SPID, CIE o CNS) e (iii) dei servizi di terze parti, quali sigilli elettronici, validazione temporale e servizio elettronico di recapito.

Il Regolamento eIDAS, tuttavia, non è stato ritenuto uno strumento idoneo al fine di affrontare le nuove richieste del mercato, in ragione delle limitazioni alla sua applicazione emerse nel corso del tempo e evidenziate dalla Commissione europea nella proposta di modifica del Regolamento eIDAS "*Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea*" del 3 giugno 2021, che ha l'obiettivo di "*migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere identità digitali affidabili per tutti gli europei*"[1]. La revisione è stata ufficialmente approvata dal Parlamento Europeo il 29 febbraio 2024 e si è in attesa del voto da parte del Consiglio per il mese di marzo, affinché sia pub-

1 Cfr. Comunicazione della Commissione, "*Plasmare il futuro digitale dell'Europa*", (COM (2020) 67 def.).

vedi l'articolo online

blicata finalmente nella Gazzetta Ufficiale nel mese di aprile 2024. Si auspica, quindi, che tra aprile e maggio 2024 entrerà in vigore la riforma del Regolamento eIDAS.

La più significativa e innovativa modifica del Regolamento eIDAS proposta della Commissione è costituita dall'implementazione di uno strumento europeo di identità digitale unico - *European Digital Identity Wallet* (in breve EUDI Wallet). L'EUDI Wallet viene definito dalla stessa Commissione europea come "*un prodotto o servizio che consente all'utente di conservare dati di identità, credenziali e attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione online e offline, per un servizio (...) nonché per creare firme elettroniche qualificate e sigilli elettronici qualificati*".

La Commissione ha ideato, dunque, un contenitore di identità pubbliche creando un sistema di riconoscimento pienamente interoperabile, di semplice utilizzo da parte dell'utente e che funziona tramite app mobili, che dovranno garantire la sicurezza delle informazioni e la protezione dei dati. In particolare, l'utente avrà il pieno controllo dei propri dati - necessari per la propria identificazione digitale e per consentire l'accesso ai servizi pubblici e privati - decidendo quali informazioni condividere e con quali soggetti. Il tutto con la garanzia che ciò avvenga in maniera sicura e riguardi solo e unicamente le informazioni necessarie ad accedere ad uno specifico servizio nel pieno rispetto dei principi di minimizzazione e necessità.

Lo scopo principale del progetto sull'EUDI Wallet proposto dalla Commissione europea è quindi quello di superare l'attuale frammentazione europea e offrire un approccio armonizzato che, grazie ad un ecosistema interoperabile, consenta ai cittadini di identificarsi online in maniera sicura e uniforme in tutta l'UE e nel pieno rispetto dei principi sanciti dalla regolamentazione di settore (tra cui il GDPR).

L'interoperabilità dell'EUDI Wallet all'interno dell'Unione Europea verrà garantita dal fatto che ciascuno Stato Membro dovrà emettere il proprio Wallet nel rispetto degli standard previsti[2] e nell'ambito di un regime nazionale di identificazione elettronica notificato alla Commissione, il cui livello di garanzia sia

2 In particolare si veda il Regolamento di esecuzione (UE) n. 2015/1501 emanato dalla Commissione ai sensi dell'articolo 12, paragrafi 2 e 8 del regolamento eIDAS , il quale stabilisce i requisiti tecnici e operativi del quadro di interoperabilità. Il regolamento di esecuzione definisce un'infrastruttura informatica che abilita la circolarità delle

elevato.[3]

2. Il Sistema di portafoglio digitale Italiano – IT-Wallet

Nell'ambito del progetto dell'EUDI Wallet e in coerenza con il cronoprogramma europeo, l'Italia ha avviato la progettazione e lo sviluppo del proprio wallet digitale, l'IT-Wallet, il cui obiettivo è quello di armonizzare la coesistenza dei tre strumenti italiani di identità digitale, parzialmente sovrapposti, a volte in competizione, basati su tecnologie differenti: SPID, CIE e CNS.

Il 2 marzo 2024 è stato pubblicato il Decreto PNRR (D.L. n. 19/2024 rubricato "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza) il quale ha ufficialmente istituito l'IT-Wallet inserendo nel Codice dell'Amministrazione Digitale ("CAD") il nuovo art. 64-quater rubricato "Sistema di portafoglio digitale italiano - Sistema IT-Wallet". Il Decreto PNRR ha in tal modo anticipato il rilascio del wallet europeo, previsto per il 2026.

Il Sistema di portafoglio digitale italiano, così come previsto per il futuro EUDI Wallet, risponde all'esigenza di passare "*dalla fornitura e dall'uso di identità digitali rigide, alla fornitura e al ricorso di attributi specifici relativi a tali identità*"[4], ossia di prerogative o qualità di una persona fisica o giuridica in formato elettronico, come i certificati medici o le qualifiche professionali. In particolare, l'utilizzo di attributi elettronici legati ad un'identità digitale permette agli utenti di gestire la condivisione dei dati di identità e limitarla a ciò che è strettamente necessario per il servizio pubblico richiesto, in ossequio al principio della minimizzazione del trattamento.

Il Sistema IT-Wallet sarà disponibile in due versioni: (i) una pubblica, accessibile a tutti i cittadini e gratuita (IT-Wallet pubblico), resa disponibile mediante l'utilizzo dell'app IO, che permetterà di conservare e utilizzare documenti digitali tra i quali, inizialmente, tessera sanitaria, patente e carta europea della

identità digitali nell'Unione europea e che consente ai cittadini di servirsi della loro eID per usufruire dei servizi erogati dai service provider pubblici e privati di tutti gli Stati membri, che prende il nome di "nodo".

3 Cfr. art. 8, del Regolamento UE n. 910/2014, sui Livelli di garanzia dei regimi di identificazione elettronica

4 Cfr. Commissione Europea, "*Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea*" del 3 giugno 2021, COM(2021) 281.

vedi l'articolo online

disabilità; (ii) una versione di portafoglio digitale privata (IT-Wallet privato), resa disponibile da soggetti privati interessati, per l'offerta di determinati servizi, previo accreditamento da parte dell'AgID.

Gli attributi possono essere quindi sia pubblici (come l'ISEE) che privati (forniti da entità private connesse all'ecosistema dell'identità digitale).

L'autenticazione tramite SPID, già prevista per l'app IO, consentendo la trasmissione al servizio dei vari attributi del cittadino, fornisce una base sicura per la gestione dei dati all'interno dell'IT-Wallet.

I cittadini potranno, quindi, utilizzare l'IT-Wallet per mostrare i documenti durante un controllo (di persona o via internet) o per accedere a servizi online (es. noleggio auto, attivazione di un servizio). Ciò in quanto i documenti presenti in questo portafoglio avranno pieno valore legale, sia per un utilizzo personale che attraverso internet.

Entro l'estate i documenti di identità selezionati - tessera sanitaria, patente e carta europea della disabilità - saranno caricabili sull'app IO, ma solo per usi "*offline*". A fine anno o inizio del 2025 l'app IO potrà essere utilizzata anche per operazioni e transazioni online.

Il nuovo art. 64-quater del CAD prevede che entro 60 giorni dovranno essere approvate con decreto delle linee guida che andranno a definire una serie di elementi al fine di "garantire la necessaria celere evoluzione del Sistema di IT-Wallet"[5], tra cui: a) le caratteristiche tecniche e le modalità di adozione dell'IT-Wallet pubblico e delle soluzioni di IT-Wallet privato da parte di cittadini e imprese, nonché la tipologia di servizi resi disponibili dalle soluzioni IT-Wallet; b) le modalità di accreditamento presso l'AgID dei soggetti privati fornitori delle soluzioni IT- Wallet privato; c) i servizi resi disponibili alle pubbliche amministrazioni e ai soggetti privati accreditati, sia in qualità di erogatori di servizi, sia in qualità di erogatori di attestazioni elettroniche relative a prerogative, caratteristiche, licenze o qualità di persone fisiche e giuridiche; d) gli standard tecnici adottati per garantire interoperabilità del Sistema IT-Wallet con le banche dati e i sistemi informativi della pubblica amministrazione e dei soggetti privati accreditati, anche al fine di garantire la compatibilità dell'IT-Wallet pubblico e delle soluzioni di IT-Wallet privato con precedenti sistemi di identità digitale e con i relativi sistemi di autenticazione per l'accesso in rete già predisposti; e) le misure da adottare sul piano tecnico e organizzativo per assicurare livelli di affidabilità, disponibilità e sicurezza adeguati al Sistema IT-Wallet; f) le modalità per la messa a disposizione del codice sorgente di tutte le componenti dell'IT- Wallet pubblico e delle soluzioni di IT-Wallet privato.

La speranza è che l'IT-Wallet non sia per i cittadini solo un diverso contenitore per le identità digitali, ma che raggiunga l'obiettivo dell'interoperabilità e della fruizione dei servizi pubblici e privati tra i diversi Stati membri dell'UE.

3. Wallet digitale: privacy e sicurezza

Il progetto del Digital Wallet presenta molteplici profili di rilievo in materia di protezione dei dati personali con particolare riferimento alla sicurezza e alla privacy by design e by default. Li andremo qui di seguito ad analizzare rifacendosi a quanto espresso dal Garante europeo (EDPS) sulle tematiche privacy[6] ed a quanto precisato dall' ENISA (Agenzia dell'Unione europea per la cybersicurezza) al fine di definire gli standard digitali di sicurezza che devono essere rispettati nello sviluppo dell'EUDI Wallet per garantirne la compliance con le politiche di cybersicurezza dell'UE.

Il Garante europeo ha sottolineato l'importanza dei principi di privacy by design e privacy by default, quali principi che devono ispirare l'intera progettazione e sviluppo del Wallet, del principio di minimizzazione del trattamento, in virtù del quale devono essere trattati solo i dati strettamente necessari al fine dell'utilizzo del Wallet e l'utente deve avere il pieno controllo sui propri dati, nonchè dei meccanismi di certificazione della compliance privacy.

Con riferimento al profilo della sicurezza il Garante ha ribadito che deve essere garantita l'adozione delle misure previste dall'art. 32 del GDPR, ma ha sollevato una problematica di non poco conto relativa alle certificazioni sulla sicurezza. Sono molti i casi, infatti, in cui i soggetti che si sono certificati per

5 Art. 64-quater, comma 3, del CAD aggiornato dal D.L. 19/2024.

6 Cfr. Intervento di Wojciech Wiewiòroski, European Data Protection Supervisor, alla "*Cybersecurity Standardisation Conference*", 7 febbraio 2023, consultabile al seguente link https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf

la sicurezza IT ai sensi di norme ISO - quali la ISO 27001 sulla sicurezza delle informazioni – abbiano l'erronea convinzione che tale certificazione garantisca automaticamente la conformità all'art. 32. È opportuno, invece, che venga scelto uno schema di certificazione specifico in materia di protezione e sicurezza dei dati personali o che vengano adottate misure ulteriori specifiche per il GDPR rispetto a quelle previste dagli schemi di certificazione per la sicurezza IT. A tal proposito l'ENISA si è proposta quale organismo di impulso e sostegno delle attività che si stanno portando avanti per la realizzazione del Wallet nell'ambito di uno standard europeo di riferimento.

Insomma sia il Garante che l'ENISA segnalano come sia indispensabile per prima cosa guadagnare la fiducia dei cittadini sullo strumento del Wallet, che potrà essere ottenuta solo garantendo un elevato livello di sicurezza sia con rifermento allo strumento in sé sia con riferimento alla protezione dei dati personali, a partire dai dati di autenticazione.

È, pertanto, indispensabile che vengano stabiliti degli standard di riferimento, che circoscrivano la tipologia di dati richiedibili all'utente e limitino le finalità di utilizzo di tali dati, che definiscano l'architettura tecnica e i meccanismi di certificazione che devono essere coinvolti nel progetto del Wallet digitale. In tal modo potrà essere garantita la compliance sia sotto il profilo del GDPR che della cybersecurity.

La proposta di revisione del regolamento eIDAS prevede che la conformità alla cybersecurity dei requisiti e delle specifiche tecniche previste per l'EUDI Wallet vengano certificate da organismi di valutazione della conformità, accreditati ai sensi del Cybersecurity Act e designati dagli Stati membri. Sulla base delle informazioni provenienti dagli Stati membri, la Commissione redige, pubblica e aggiorna un elenco degli EUDI wallets certificati. Probabilmente il ruolo di ente certificatore della sicurezza dell'EUDI Wallet verrà affidato all'ENISA.

Per quanto riguarda la sicurezza dei sistemi di Digital Identity Wallet, essa dovrà essere garantita in relazione sia al riconoscimento dell'utente sia alla conservazione delle informazioni del cittadino. A tal proposito si stanno studiando diverse soluzioni, dall'utilizzo di *secure elements* dei diversi sistemi operativi degli smartphone, a soluzioni miste, che prevedono il supporto di componenti in cloud rispetto all'utilizzo del solo wallet.

Dello stesso avviso è anche il Consiglio dell'OECD (*Organisation for Economic Co-operation and Development*) che, nelle raccomandazioni su come governare il sistema di identità digitale, pubblicate l'8 giugno 2023,[7] ha esortato gli Stati a proteggere la privacy e dare la priorità alla sicurezza per garantire la fiducia dei cittadini europei verso i sistemi di identità digitale. A tal proposito, potrebbe essere implementata l'autenticazione mediante dati biometrici, in quanto tale tecnica, combinata con altri elementi di autenticazione, garantisce un elevato livello di sicurezza.

Gli Stati dovranno quindi collaborare nello stabilire requisiti comuni, compresi i requisiti di sicurezza informatica, in modo tale da tutelare i diritti degli utenti e delle parti interessate e dovranno impegnarsi nella cooperazione normativa internazionale per consentire l'interoperabilità transfrontaliera dei sistemi di identità digitale.

Un primo esempio sulle modalità di sicurezza da implementare al fine di governare un sistema di Digital Identity Wallet lo avremo in Italia, quando saranno emanate le linee guida previste dall'art. 64-quater comma 3 del CAD. Infatti si prevede che tali linee guida andranno a definire, tra le altre cose, anche gli standard tecnici che dovranno essere adottati per garantire l'interoperabilità del Sistema IT-Wallet con le banche dati e i sistemi informativi della pubblica amministrazione e dei soggetti privati, nonché le misure da adottare sul piano tecnico e organizzativo per assicurare livelli di affidabilità, disponibilità e sicurezza adeguati.

Ci si chiede infine come IT e EUDI Wallet si relazioneranno una volta che saranno entrambi operativi. Non resta che attendere le fasi di sviluppo del progetto con l'auspicio che si realizzi l'interoperabilità digitale perseguita dalla Commissione europea.

7 OECD, "*Recommendation of the Council on the Governance of Digital Identity*", 8 giugno 2023. Consultabile al seguente link: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it