Il diritto digitale
Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

IL DIRITTO DIGITALE
Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

Title: LEGAL DESIGN AND DATA SCIENCE FOR EXPLICABLE AI IN LEGAL DOMAIN
Acronym: LEDS 4 XAIL
n. GPA: 101085576
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Fondazione Bologna University Press
Via Saragozza 10, 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
e-mail: info@buponline.com

ISBN 979-12-5477-771-8
ISBN on line 979-12-5477-772-5
DOI 10.30682/9791254777725

Questo volume è stato realizzato a partire da un impaginato camera-ready in formato pdf fornito dai curatori

In copertina: Summit Art Creations/Shutterstook.com

Prima edizione: marzo 2026

INDICE

Introduzione 1
Federico Galli, Monica Palmirani, Salvatore Sapienza, Giovanni Sartor

PARTE I – DATI

La protezione dei dati personali 11
Federico Galli, Giovanni Sartor

Data Governance Act e Data Act nel quadro degli Spazi Comuni Europei dei Dati 37
Salvatore Sapienza

L'uso secondario dei dati sanitari elettronici nella cornice dell'European Health Data Space 55
Paola Aurucci

Open Government Data 75
Monica Palmirani

Investigare i dati informatici: la *digital forensics* tra norme giuridiche, standard tecnici e innovazioni tecnologiche 97
Raffaella Brighi, Michele Ferrazzano

PARTE II – STRUMENTI ABILITANTI

Identità e firme digitali 121
Chantal Bomprezzi, Monica Palmirani

Smart contract e blockchain 137
Chantal Bomprezzi

PARTE III – SISTEMI E PRODOTTI

La protezione dei beni informatici attraverso il diritto d'autore 161
Claudio Di Cocco

La regolazione dell'Intelligenza Artificiale nell'UE: l'AI Act 203
Giuseppe Contissa, Marco Billi

La decisione automatica e la sua spiegazione tra GDPR e AI Act 221
Francesca Lagioia, Giovanni Sartor

Responsabilità e Intelligenza Artificiale 251
Chantal Bomprezzi

PARTE IV – MERCATI E SERVIZI

La regolazione dei mercati digitali: il Digital Markets Act 263
Federico Galli

La regolazione degli intermediari di Internet: il Digital Service Act 287
Giuseppe Contissa

La tutela del consumatore digitale 307
Federico Galli

PARTE V – SICUREZZA

La Cybersicurezza nella trasformazione digitale 341
Raffaella Brighi

Il diritto UE della Cybersicurezza: il quadro normativo 363
Pier Giorgio Chiara

I reati informatici e la violazione dei diritti della persona in rete 391
Francesco Di Tano

Il data breach e l'incidente di sicurezza 409
Juri Monducci

PARTE VI – ETICA DEL DIGITALE

Etica dell'Intelligenza Artificiale 435
Giorgio Bongiovanni, Claudio Novelli

Gli Autori 463

IDENTITÀ E FIRME DIGITALI

*Chantal Bomprezzi, Monica Palmirani**

Sommario: 1. Quadro normativo. 2. Il documento informatico, le firme elettroniche e l'equivalenza funzionale. 3. Le tipologie giuridiche di firma elettronica. 4. Il valore giuridico e probatorio dei documenti elettronici e delle firme elettroniche. 5. Servizi fiduciari e certificatori. 6. L'identità digitale 7. Portafoglio europeo d'identità digitale (*EUDI Wallet*) 7.1. *(Segue)*: EUDI Wallet e identità digitale auto-sovrana (SSI) 8. La frammentazione dell'*identity management* nell'UE 9. L'interoperabilità nei servizi della Pubblica amministrazione

1. Quadro normativo

L'Italia è stata tra i primi Paesi a dotarsi di un quadro normativo sui documenti informatici e le firme elettroniche. Ci si riferisce, in particolare, alla Legge 15 marzo 1997, n. 59 ("Delega al Governo per il conferimento di funzioni e compiti alle Regioni ed agli Enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa"), che all'art. 15, co. 2, disponendo che «gli atti, i dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con documenti informatici, sono validi e rilevanti a tutti gli effetti di legge», introduceva una regolamentazione organica sulla validità e rilevanza giuridica delle rappresentazioni informatiche di documenti. La specifica normativa sulle firme elettroniche è, invece, di derivazione comunitaria e si deve per la prima volta alla Direttiva 1999/93/CE, poi attuata in Italia con il d.lgs. 10/2002.

Queste disposizioni sono successivamente state abrogate, riordinate e consolidate all'interno del d.lgs. 7 marzo 2005, n. 82, o "Codice dell'Amministrazione digitale" (da qui in avanti, CAD). Il CAD è stato modificato a più riprese nel corso degli anni, anche per adeguarsi alle più recenti disposizioni europee del Regolamento UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (d'ora in avanti, Reg. eIDAS). Quest'ultimo Regolamento è nato per garantire il buon funzionamento del mercato interno, rafforzando la fiducia nelle transazioni elettroniche, fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'*eBusiness* e del commercio elettronico, nell'Unione europea. L'obiettivo del Regolamento è quello di garantire l'interoperabilità giuridica e tecnica tra gli Stati membri dell'UE riguardo agli strumenti elettronici di identificazione, autenticazione e firma, migliorando così l'efficacia dei servizi online all'interno dell'Unione europea.

* Pur senza tradire l'unitarietà del lavoro, alla Dott.ssa Bomprezzi vanno attribuiti i paragrafi da 1 a 7, e alla Prof.ssa Palmirani i paragrafi da 7.1 a 9.

La natura di Regolamento (e non di Direttiva) dell'eIDAS ha consentito al medesimo di essere direttamente applicabile in tutti gli Stati membri, scongiurando così la frammentazione normativa e favorendo l'armonizzazione del diritto nel mercato unico. Le modifiche al CAD, come testé accennato, sono appunto servite per raccordare la disciplina italiana con quella europea.

La disciplina introdotta dal CAD (la quale, a discapito di quanto il nome possa suggerire, si applica anche ai privati (ove non diversamente previsto) è integrata da Linee guida contenenti le regole tecniche (art. 71) aventi la duplice funzione di dettagliare le norme generali e di favorire l'aggiornamento dettato dall'evoluzione tecnologica.

Da ultimo, il Regolamento eIDAS è stato modificato e aggiornato nel 2024 mediante il Regolamento UE 2024/1183 (detto anche "eIDAS 2"). Le principali novità di tale revisione hanno riguardato l'introduzione del Portafoglio di identità digitale europea (o "*EUDI Wallet*") e altri nuovi servizi fiduciari come i registri elettronici e l'archiviazione elettronica a lungo termine.

2. Il documento informatico, le firme elettroniche e l'equivalenza funzionale

Il documento informatico è definito all'art. 1, lett. p, del CAD come «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». Ai sensi dell'art. 3, par. 1, n. 35, del Reg. eIDAS, il documento elettronico è «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva».

Secondo il principio di non discriminazione, esplicitato all'art. 46 del Reg. eIDAS, a un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali – così come accade per i documenti cartacei – per il solo motivo della sua forma elettronica.

Il documento informatico si sostanzia in una sequenza di *bit* ed è il risultato di un'elaborazione informatica. La funzione è la medesima del documento cartaceo, e consiste nel rappresentare atti, fatti o dati giuridicamente rilevanti. A questa conclusione si è pervenuti a seguito di un vivace dibattito dottrinale, dettato dall'avvento delle nuove tecnologie e dal passaggio dal documento cartaceo a quello informatico. A tal proposito, illuminante è l'insegnamento di Carnelutti, il quale riteneva documento «qualsiasi cosa idonea a far conoscere un fatto», sostenendo l'irrilevanza della materia di cui lo stesso fosse composto. Egli affermava, difatti, che «qualunque materia, at-

ta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo»[1].

Al pari del documento, anche tra firma autografa e firma elettronica non deve sussistere discriminazione. L'art. 25 del Reg. eIDAS prescrive all'uopo che «A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica». Invero, seppure firma cartacea ed elettronica abbiano natura diversa (l'una basandosi sulla grafia ed essendo il risultato di un gesto umano, l'altra essendo il risultato di una procedura tecnologica), da un punto di vista giuridico occorre guardare all'idoneità della firma elettronica ad assolvere alle medesime funzioni della sottoscrizione (principio di equivalenza funzionale).

Le funzioni della sottoscrizione autografa sono tre[2]: indicativa, che consiste nell'identificare l'autore del documento; dichiarativa, che prevede che la sottoscrizione imputi al titolare del nome la paternità del documento; probatoria, per cui la sottoscrizione prova la provenienza del documento. A seconda della tipologia di firma elettronica utilizzata e della capacità di assolvere a queste funzioni, il legislatore o il giudice (a seconda dei casi) stabiliscono l'equivalenza alla firma autografa.

3. Le tipologie giuridiche di firma elettronica

La firma elettronica viene definita all'art. 3, par. 1, n. 10, del Reg. eIDAS come «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare». L'art. 1, lett. aa, del CAD identifica il firmatario come «la persona *fisica* cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione, nonché alle applicazioni per la sua apposizione».

Le firme elettroniche sono giuridicamente distinte in quattro tipologie, caratterizzate da un progressivo grado di maggiore sicurezza circa la capacità di assolvere alle funzioni della firma autografa: 1) semplice; 2) avanzata; 3) qualificata; 4) digitale.

La firma elettronica semplice corrisponde alla definizione di firma elettronica fornita pocanzi. Un esempio di firma elettronica semplice potrebbe essere rappresentato dalla *e-mail*, o posta elettronica semplice.

La firma elettronica avanzata è una firma elettronica semplice che soddisfa i requisiti di cui all'art. 26 Reg. eIDAS (v. art. 3, par. 1, n. 11, Reg.). I requisiti so-

[1] F. CARNELUTTI, *Documento – teoria moderna*, in *Noviss. Dig. it.*, 1957 (VI), p. 85 ss.; *Id.*, *Documento e negozio giuridico*, in *Riv. dir. proc. civ.*, 1926 (I), p. 181 ss.

[2] F. CARNELUTTI, *Studi sulla sottoscrizione*, in *Riv. Dir. Comm*, 1929 (IX-X), pp. 509 ss.

no: a) essere connessa unicamente al firmatario; b) essere idonea a identificare il firmatario; c) essere 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) essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati. Un esempio di firma elettronica avanzata potrebbe consistere nella firma grafometrica, la quale corrisponde a una sottoscrizione autografa apposta su un tablet informatico con una particolare penna.

La firma elettronica qualificata, ex art. 3, par. 1, n. 11, Reg. è una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. I requisiti ulteriori che una firma elettronica deve avere per essere considerata qualificata sono dunque due: l'apposizione mediante un dispositivo apposito, che deve rispettare i requisiti prescritti dall'allegato II del Reg. eIDAS; la presenza di un certificato qualificato rilasciato da un prestatore di servizi fiduciari qualificato conforme ai requisiti di cui all'allegato I del Reg. eIDAS. A titolo esemplificativo, una firma qualificata può essere quella apposta con *smart card* o dispositivo USB. Esistono anche tipologie di firma elettronica qualificata "remota", che prescinde dal rilascio di un dispositivo fisico.

Per la firma elettronica qualificata, ex art. 24 bis, par. 1, Reg. si applica il principio del reciproco riconoscimento, ovvero che le firme elettroniche qualificate basate su un certificato qualificato rilasciato in uno Stato membro sono riconosciute come firme elettroniche qualificate in tutti gli altri Stati membri. La finalità sottesa a tale principio è evidentemente quella di favorire la diffusione di questi strumenti nel mercato dell'UE.

Infine, la firma digitale è un particolare tipo di firma qualificata, caratterizzata da una specifica tecnologia. Per questo tipo di firma, dunque, non si applica il principio della neutralità tecnologica. Mentre secondo quest'ultimo principio, cioè, è indifferente la tecnologia utilizzata (rilevando esclusivamente il soddisfacimento di una serie di condizioni normative), la firma digitale è basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. La firma digitale è una tipologia di firma tipicamente italiana, non definita dal Reg. eIDAS, bensì dal CAD (art. 1, lett. s). Per le sue caratteristiche, tuttavia, viene ricompresa all'interno delle firme elettroniche qualificate.

4. Il valore giuridico e probatorio dei documenti elettronici e delle firme elettroniche

I documenti informatici assumono un diverso valore giuridico e probatorio a seconda che siano privi di firma elettronica o sottoscritti con le varie tipologie giuridiche di firma elettronica (semplice, avanzata, qualificata, digitale).

Il documento informatico sprovvisto di firma, come già visto[3], è valido ed efficace giuridicamente. L'art. 20, co.1-*bis*, del CAD statuisce che l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità. Sono dunque affidati alla discrezionalità del giudice, caso per caso, il valore e l'efficacia del documento, in base alle caratteristiche dello stesso. Questa regola si applica anche in caso di documento informatico firmato con firma elettronica semplice.

La medesima norma riconosce, invece, al documento informatico firmato con firma elettronica avanzata, qualificata e digitale il soddisfacimento del requisito della forma scritta e l'efficacia prevista dall'art. 2702 c.c.

Parimenti, lo stesso vale anche quando il documento è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AGID (l'Agenzia per l'Italia Digitale) ai sensi dell'art. 71 (del CAD) con modalità tali da garantire la sicurezza, l'integrità e l'immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. Trattasi della c.d. "firma tramite SPID" (su cui si veda *infra*).

In queste ipotesi, dunque, la discrezionalità del giudice viene meno (ex art. 2702 c.c. la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta) e l'equivalenza funzionale tra firma autografa ed elettronica è espressamente sancita dalla legge, seppur con dei distinguo a seconda del tipo di documento da firmare. Nello specifico, ex art. 21, co. 2-*bis*, CAD, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o firma digitale. Gli atti di cui all'art. 1350, numero 13, del Codice redatti su un documento informatico sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale, ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-*bis*, primo periodo (firma con SPID).

Per sintetizzare, la firma elettronica semplice è idonea alla firma di contratti e atti non formali (come ad esempio preventivi, lettere di incarico, moduli di acquisizione del consenso al trattamento dei dati personali); la firma elettronica

[3] Vedi *supra*, par. 2.

avanzata e la firma tramite SPID prevedono un ambito di applicazione più ampio, che si estende anche agli atti e contratti *non* aventi ad oggetto beni immobili che richiedono la forma scritta *ad substantiam*, di cui all'art. 1350, n. 13, c.c. (vi ricadono, ad esempio, i contratti bancari) o i contratti che richiedono la forma scritta *ad probationem* (come i contratti assicurativi); infine, un ambito di applicazione massimo è riconosciuto alla firma elettronica qualificata e digitale, apponibile a qualunque contratto, anche avente ad oggetto beni immobili che richiedono la forma scritta *ad substantiam* ex art. 1350, n. da 1 a 12, c.c.

Una particolarità è rappresentata, poi, dall'art. 20, co. 1-*ter*, CAD, a mente del quale «L'utilizzo del dispositivo di firma elettronica *qualificata* o *digitale* si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria», con un'inversione dell'onere della prova normalmente prescritto per l'analogo documento cartaceo (ex art. 214 c.p.c.). Tramite questo meccanismo, la funzione probatoria del documento firmato con firma elettronica qualificata o digitale è rafforzata, poiché spetterà al titolare della firma, che la voglia disconoscere, a dover dimostrare in giudizio di non aver firmato. Il disconoscimento, qui, ha ad oggetto non la sottoscrizione, ma il dispositivo, in quanto, di base, la firma qualificata o digitale è per natura sempre vera e integra, essendo posta in atto con un dispositivo. Si passa da un criterio di "paternità" della firma autografa ad uno di "responsabilità" della firma elettronica qualificata o digitale[4] (accompagnato, ex art. 32 CAD, da un corrispondente obbligo di custodia del dispositivo di firma da parte del titolare, il quale è altresì tenuto ad utilizzare personalmente il suddetto dispositivo).

5. Servizi fiduciari e certificatori

La firma qualificata garantisce la connessione univoca tra la firma e il firmatario grazie alla presenza di un certificato qualificato che lo attesta. Un certificato qualificato di firma elettronica è un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona, rilasciato da un prestatore di servizi fiduciari qualificato e conforme ai requisiti di cui all'allegato I del Regolamento eIDAS (art. 3, par. 1, n. 14 e 15).

I servizi fiduciari sono servizi elettronici, forniti normalmente dietro remunerazione, che divengono qualificati nel momento in cui offrono servizi fiduciari qualificati (art. 3, par. 1, n. 16 e 17) e la cui valutazione di conformità è effettuata da un apposito organismo accreditato a norma del Regolamento (art. 3, par. 1, n. 18). In Italia, tali organismi sono accreditati da ACCREDIA. I presta-

[4] Questa diversità di criteri è stata affermata dal Consiglio di Stato, Sezione Consultiva per gli Atti Normativi, nell'adunanza del 7 febbraio 2005.

tori di servizi fiduciari qualificati sono soggetti a vigilanza da parte di un organismo istituzionale nazionale (in Italia, l'Agenzia per l'Italia Digitale, o AGID), a cui per avviare il servizio qualificato occorre notificare una relazione di valutazione della conformità al regolamento e agli atti di esecuzione rilasciata dall'organismo di valutazione della conformità. La verifica dell'organismo di valutazione della conformità va ripetuto ogni 24 mesi per mantenere lo status, e poi l'esito della valutazione va comunicato ad AGID.

L'elenco dei prestatori è pubblico[5]. Per rilasciare il dispositivo e il certificato qualificato di firma, il prestatore di servizio fiduciario qualificato deve identificare a monte il soggetto richiedente in modo rigoroso (ad esempio tramite SPID o di persona).

Occorre sempre verificare la validità del certificato qualificato, escludendo che esso sia scaduto, revocato o sospeso. La revoca è l'operazione con cui il certificatore annulla la validità del certificato (ad esempio, per morte del titolare), mentre la sospensione ne sospende la validità per un determinato periodo di tempo (ad esempio, per furto). L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione (art. 24, co. 4-*bis*, CAD).

6. L'identità digitale

Con l'avvento di Internet si è posto con forza il tema dell'identità digitale e dell'identificazione online. Emblematica la famosa vignetta di Peter Steiner pubblicata sul periodico *The New Yorker* del 5 luglio 1993, raffigurante un cane seduto su una sedia davanti ad un computer che dice al cane a fianco a sé: «*On the Internet, nobody knows you're a dog*» («Su Internet, nessuno sa che sei un cane»). Conoscere l'identità di un soggetto (i.e., poterlo identificare) è giuridicamente rilevante, a volte prescritto dalla legge. Il problema si pone quando si tratta di dover identificare in maniera certa qualcuno a distanza, *online*.

Il Regolamento eIDAS interviene anche su questo aspetto. Anzitutto, esso distingue tra "identificazione elettronica" e "autenticazione elettronica". Con la prima, si intende «il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta un'altra persona fisica o una persona giuridica» (art. 3, par. 1, n. 1); con la seconda, «un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure di confermare l'origine e l'integrità di dati in forma elettronica» (art.

[5] https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls.

3, par. 1, n. 5). Il Regolamento, poi, consente agli Stati membri di notificare alla Commissione europea degli strumenti di identificazione online, a certe condizioni (art. 7), che, se accettati dalla Commissione e pubblicati, devono essere riconosciuti come tali in tutti gli altri Stati membri (secondo il principio del mutuo riconoscimento di cui all'art. 6). Tali sistemi di identificazione elettronica sono distinti in livelli di garanzia, a seconda del grado di fiducia che forniscono circa l'identità dichiarata. I livelli si distinguono, ex art. 8, in basso, significativo ed elevato. In caso di livello basso, gli enti pubblici hanno la facoltà di riconoscimento ai fini dell'autenticazione transfrontaliera. Se invece, il livello di garanzia è pari o superiore al livello richiesto dall'organismo del settore pubblico, e se è almeno significativo o elevato, sussiste l'obbligo di riconoscimento. Queste norme valgono e sono obbligatorie in caso di identificazione presso un soggetto pubblico; permangono una facoltà per i soggetti privati.

L'Italia ha notificato lo SPID e la CIE. SPID sta per Sistema Pubblico d'Identità Digitale, e consente a ogni cittadino di ottenere la propria identità digitale tramite cui accedere con un'unica credenziale (*username* e *password*), ai servizi digitali delle Pubbliche amministrazioni degli Stati membri. La CIE è la Carta d'Identità Elettronica, emessa dal Ministero dell'Interno come documento di identificazione e utilizzabile anche per accedere ai servizi online.

Oltre i confini europei, il mutuo riconoscimento delle identità digitali è favorito dai principi statuiti, seppur solo a livello di *soft law*, dal *Working Group IV* sul Commercio elettronico dell'UNCITRAL, che ha elaborato un apposito *Model Law*[6].

7. Portafoglio europeo d'identità digitale (*EUDI Wallet*)

Tra i nuovi servizi fiduciari introdotti dal Regolamento eIDAS 2 vi è il portafoglio europeo d'identità digitale (o *European Digital Identity Wallet*, altrimenti detto *EUDI Wallet*).

Il portafoglio europeo di identità digitale è definito come «un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati» (art. 3, n. 42).

[6] *Model Law on the Use and Cross-border Recognition on Identity Management and Trust Services*, https://uncitral.un.org/en/mlit.

Il portafoglio europeo di identità digitale rappresenta una delle novità più significative derivanti dalla revisione del Regolamento eIDAS, in linea con l'obiettivo di fornire ai cittadini dell'Unione, seppur in via facoltativa, un'identità digitale che sia sotto il loro controllo esclusivo e ovviare così alla gestione di numerose credenziali, *password* e *account* in mano ai prestatori dei servizi *online*. La peculiarità del portafoglio europeo, infatti, è la divulgazione selettiva dei dati personali da parte dell'utente e sotto il proprio esclusivo controllo (v. cons. 15), al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso transfrontaliero sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati (art. 5-*bis*).

Lo stesso art. 5-*bis* detta come limite temporale la fine del 2026 affinché ciascuno Stato membro fornisca almeno un portafoglio europeo di identità digitale. Questi possono essere forniti: direttamente dallo Stato membro; su incarico di uno Stato membro; indipendentemente da uno Stato membro pur essendo riconosciuti da quest'ultimo (art. 5-*bis*, par. 2). Il codice sorgente dei componenti *software* dell'applicazione deve essere caratterizzato da una licenza open source (art. 5-*bis*, par.3). Il livello di garanzia del mezzo di identificazione elettronica deve essere elevato (art. 5-*bis*, par. 11).

Qualora il portafoglio venga usato per firmare, occorre offrire a tutte le persone fisiche la possibilità di apporre firme elettroniche qualificate per impostazione predefinita e gratuitamente, limitatamente a scopi non professionali (art. 5-*bis*, par. 5, lett. g)).

La conformità dei portafogli europei di identità digitale ai requisiti prescritti è certificata da organismi di valutazione della conformità designati dagli Stati membri e comunicati alla Commissione. La certificazione è valida fino a cinque anni, a condizione che sia effettuata una valutazione di vulnerabilità ogni due anni (art. 5-*quater*). È prevista da parte della Commissione la pubblicazione di un elenco dei portafogli europei di identità digitale certificati (art. 5-*quinquies*).

Qualora gli Stati membri richiedano l'identificazione e l'autenticazione elettroniche per accedere a servizi online prestati da un organismo del settore pubblico, essi debbono accettare anche i portafogli europei di identità digitale forniti conformemente al Regolamento (art. 5-*septies*).

In Italia, il Sistema di portafoglio digitale italiano, o *IT-Wallet*, disciplinato dall'art. 64-*quater* del CAD, e integrato nell'app IO, è la versione italiana che anticipa l'*EUDI Wallet*, e che dovrà conformarsi agli *standard* del Regolamento eIDAS per divenire compatibile e interoperabile con il sistema europeo.

7.1. (*Segue)*: EUDI Wallet e identità digitale auto-sovrana (SSI)

L'EUDI Wallet introduce nuove opportunità per promuovere l'eguaglianza tra diverse categorie di cittadini. In alcune implementazioni nazionali, ad esempio, la Disability Card europea è stata integrata nel portafoglio digitale nazionale (come nel caso spagnolo e nell'applicazione IO in Italia), e gli studenti possono caricare le proprie tessere universitarie digitali. Tuttavia, il regolamento eIDAS 1.0 presenta taluni elementi suscettibili di attuazione in modo non pienamente conforme al principio di minimizzazione dei dati (*privacy by default*). La riforma introdotta con eIDAS 2.0 e l'EUDI Wallet è volta precisamente a colmare tali lacune.

Nella procedura ordinaria di identificazione digitale, il regolamento eIDAS 1.0 individua almeno tre attori principali: (i) il fornitore di identità (*identity provider*), (ii) il fornitore di servizi (*service provider*) e (iii) il prestatore di attributi qualificati. In tale quadro procedurale, lo standard tecnico Security Assertion Markup Language (SAML) disciplina lo scambio dei soli dati strettamente necessari all'identificazione dell'utente. In conformità al principio di minimizzazione dei dati, sancito dall'articolo 5, paragrafo 1, lettera c), del GDPR, il fornitore di identità e il prestatore di attributi sono a conoscenza dell'identità del soggetto che richiede il servizio; tuttavia, tale informazione dovrebbe essere opportunamente schermata al fine di evitare divulgazioni indebite tramite metadati.

Ciononostante, in diverse implementazioni nazionali tale obbligo di mascheramento non viene rispettato, poiché il regolamento eIDAS 1.0 consente tecnicamente questo approccio (come nel caso dello SPID in Italia). Ne consegue che soggetti terzi possono desumere quali servizi pubblici siano stati utilizzati dall'utente, ad esempio servizi sanitari o richieste relative al casellario giudiziale. Tali prassi sollevano rilevanti criticità in ordine al rispetto del principio di minimizzazione sancito dal diritto europeo in materia di protezione dei dati personali. In taluni ordinamenti, l'assenza di un adeguato mascheramento può persino agevolare l'impiego di tali informazioni a fini di profilazione, consentendo l'offerta di servizi commerciali mirati o ampliati, in potenziale contrasto con le garanzie poste a tutela dei diritti fondamentali.

Il Portafoglio Europeo di Identità Digitale (EUDI Wallet) è stato introdotto dal regolamento eIDAS 2.0 proprio al fine di rafforzare il controllo dell'utente finale sulla comunicazione dei metadati relativi all'identità ai fornitori di servizi. Tale strumento consente, infatti, l'instaurazione di un regime di identità autosovrana (*self-sovereign identity*), nel quale l'interessato mantiene un controllo effettivo sul trattamento dei propri dati personali. In tal modo, l'EUDI Wallet rende concretamente operante il principio di minimizzazione dei dati, promuovendo

al contempo un approccio incentrato sul cittadino e favorendo un modello decentrato di gestione dell'identità digitale.

L'Architecture and Reference Framework (ARF) dell'EUDI Wallet specifica ulteriormente le modalità tecniche e organizzative per la gestione, all'interno di un unico strumento, di molteplici documenti e attributi digitali — quali, ad esempio, patente di guida, documentazione sanitaria o passaporto digitale — garantendo che, durante le transazioni di credenziali, non vengano divulgati metadati non necessari. In questa prospettiva, l'EUDI Wallet costituisce una nuova infrastruttura giuridico-tecnica volta ad attribuire sia alle persone fisiche sia alle persone giuridiche un maggiore controllo sui propri dati personali. Esso consente la gestione sicura e la divulgazione selettiva dei dati identificativi personali (PID), unitamente alle attestazioni elettroniche di attributi (EAAs), rafforzando la conformità ai principi di protezione dei dati e accrescendo la fiducia nei servizi digitali pubblici e privati.

Gli attori coinvolti nel sistema sono: il titolare (*holder*) dell'identità digitale europea, ossia l'interessato; il fornitore del *wallet*; il prestatore di attestazioni di attributi, qualificati e non qualificati (autorità EAAs); e il verificatore (o *relying party*), destinatario delle attestazioni.

Lo scenario operativo può essere così descritto:

Un utente (il "titolare") intende condividere talune informazioni digitali per accedere a un servizio di eGovernment (ad esempio, il livello di istruzione richiesto per partecipare a una selezione pubblica).

Un servizio pubblico o privato (il "verificatore") richiede la prova di specifici attributi (ad esempio, esclusivamente il titolo di studio) e può accettare soltanto dati provenienti da fonti ritenute affidabili (ad esempio, un'università).

Il *wallet* del titolare seleziona automaticamente le attestazioni elettroniche pertinenti (ad esempio, il diploma rilasciato dall'università).

Con il consenso dell'interessato, il *wallet* genera una "presentazione verificabile", ossia un pacchetto sicuro contenente i dati richiesti, e lo trasmette al verificatore.

In sostanza, l'EUDI Wallet attribuisce all'utente il potere di decidere quali dati condividere, con chi e in quale momento, senza il ricorso a ulteriori intermediari.

Il *wallet* si fonda sui principi dell'identità auto-sovrana (SSI). Tale mutamento di paradigma riflette e rafforza i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata (art. 7) e il diritto alla protezione dei dati personali (art. 8). Più in generale, l'EUDI Wallet incarna il principio di autodeterminazione informativa, elaborato in sede di giurisprudenza costituzionale — in modo emblematico dalla Corte costituzionale federale tedesca — secondo cui l'individuo deve poter de-

terminare quando, in quale misura e a quali condizioni i propri dati personali possano essere comunicati e trattati.

Diversamente dai modelli centralizzati basati su banche dati uniche, l'EUDI Wallet consente agli utenti di conservare attributi cifrati rilasciati da autorità pubbliche competenti. Tali attributi — che possono riguardare, ad esempio, la maggiore età, lo status di beneficiario di una prestazione o informazioni sanitarie — possono essere presentati in modo granulare e sicuro. Così, un soggetto chiamato a dimostrare la propria maggiore età potrà comunicare esclusivamente tale attributo, senza rivelare informazioni accessorie quali nome o indirizzo. Questo meccanismo di divulgazione selettiva rafforza il rispetto del principio di minimizzazione dei dati, accrescendo al contempo l'autonomia dell'utente e la fiducia nelle transazioni digitali.

L'articolo 5 del regolamento (UE) 2024/1183 garantisce l'uso di pseudonimi nelle transazioni elettroniche relative ai metadati e all'EUDI Wallet. Tuttavia, l'EUDI-ARF non è ancora in grado di fornire specifiche tecniche definitive, anche a causa dell'assenza di un quadro normativo pienamente armonizzato nei singoli Stati membri. In tale contesto, il *legal design* può supportare i decisori pubblici nel comprendere l'importanza dell'introduzione dello pseudonimo attraverso un approccio situazionale o prospettico, evidenziandone vantaggi e criticità nei diversi ordinamenti nazionali. Parimenti, il *legal design* può agevolare i cittadini nella comprensione delle innovazioni introdotte dall'EUDI Wallet rispetto ai precedenti strumenti di identificazione digitale, mediante fumetti, animazioni, mappe concettuali e simulazioni visuali delle operazioni. In questa direzione si collocano le iniziative intraprese dalla Commissione europea attraverso portali informativi dedicati.

L'EUDI Wallet integra altresì garanzie tecnologiche volte a rafforzare la cybersicurezza. In particolare, esso si coordina con la direttiva NIS2 al fine di assicurare il principio dell'accesso digitale sicuro ai servizi pubblici. Coerentemente con il regolamento (UE) 2024/1183, l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) è stata incaricata di sostenere la certificazione degli EUDI Wallet, inclusa la predisposizione di un potenziale schema europeo di certificazione della cybersicurezza nell'ambito del Cybersecurity Act (regolamento (UE) 2019/881). Attraverso tali misure, l'EUDI Wallet risulta maggiormente resiliente rispetto ad attacchi informatici e frodi, contribuendo a rafforzare la fiducia dei cittadini nell'utilizzo dei servizi pubblici digitali.

Allo stato attuale dello sviluppo tecnologico, l'EUDI Wallet integra dunque tanto i principi del GDPR quanto i pilastri fondamentali del diritto europeo in materia di cybersicurezza. Tale convergenza consente di conciliare l'esigenza di garantire un accesso sicuro ai servizi pubblici digitali con la tutela dei diritti alla riservatezza e alla protezione dei dati personali. In questa prospettiva, l'EUDI

Wallet rappresenta un esempio significativo di progettazione regolatoria capace di armonizzare sicurezza e diritti fondamentali, contribuendo alla legittimazione e alla sostenibilità del quadro europeo dell'identità digitale.

8. La frammentazione dell'*identity management* nell'UE

Gli attuali strumenti europei di identità digitale sviluppati in conformità al regolamento eIDAS 2.0, inclusi il Portafoglio Europeo di Identità Digitale (EUDI Wallet), non risultano pienamente idonei a rendere operativi meccanismi di delega strutturati e giuridicamente robusti. Un regime di delega conforme ai principi dello Stato di diritto richiederebbe, quantomeno, l'istituzione di un registro dei rappresentanti autorizzati, la definizione puntuale dell'ambito oggettivo e della durata della delega, nonché l'individuazione dei servizi pubblici cui essa si applica. Inoltre, le amministrazioni pubbliche dovrebbero adeguare i propri sistemi informatici per consentire l'accesso delegato, circostanza che implica interventi complessi sia sul piano normativo sia su quello tecnico-organizzativo.

L'attivazione dell'EUDI Wallet è rimessa alla libera scelta del cittadino. Tale opzione progettuale mira a prevenire fenomeni di esclusione digitale e a scongiurare forme di discriminazione derivanti dall'imposizione di una specifica soluzione tecnologica. L'articolo 5a, paragrafo 15, del quadro regolatorio di riferimento sancisce espressamente tale principio, garantendo al contempo la permanenza di meccanismi alternativi di identificazione e autenticazione. Se, da un lato, questa previsione attua un approccio multicanale, idoneo ad accogliere una pluralità di strumenti di identità digitale, dall'altro lato essa contribuisce a mantenere un certo grado di frammentazione nel mercato europeo della gestione dell'identità.

Attualmente, infatti, l'*identity management* nell'Unione europea si presenta ancora fortemente frammentato, configurando un settore ad elevato valore tecnologico ed economico. In tale contesto, le proposte volte all'adozione di un'identità digitale europea unificata (EUDI) intendono superare tale dispersione. La natura facoltativa dell'EUDI Wallet garantisce flessibilità nell'integrazione di diverse soluzioni tecniche e applicative, ampliando l'accessibilità e favorendo l'inclusione. Tuttavia, questa stessa impostazione inclusiva pone criticità in relazione all'effettiva interoperabilità dei servizi pubblici transfrontalieri all'interno dell'Unione. Si rende pertanto necessario un periodo transitorio volto alla standardizzazione e armonizzazione dell'EUDI, al fine di assicurare coerenza tecnica e ampia fruibilità nei diversi Stati membri.

Particolarmente significativi risultano, in questa prospettiva, gli esiti del progetto DC4EU, che ha prodotto materiali divulgativi e tecnici quali video, schede

grafiche, brochure destinate alle amministrazioni pubbliche e approfondimenti specialistici rivolti agli esperti e alle imprese. Gli obiettivi perseguiti erano molteplici: (i) rafforzare la fiducia dei cittadini; (ii) sostenere l'interoperabilità tra servizi pubblici; (iii) supportare gli attori dell'ecosistema EUDI Wallet nell'implementazione di soluzioni di *user experience* (UX) efficaci e coerenti.

Di rilievo è altresì l'iniziativa promossa da Lissicompany, volta alla creazione di un sistema di icone finalizzato a rendere l'esperienza utente più intuitiva, accessibile e interoperabile tra diversi servizi pubblici e ordinamenti nazionali. Analogo sistema iconografico è stato adottato anche da operatori quali Maggioli per l'offerta dell'EUDI Wallet in Italia, contribuendo alla diffusione di standard comunicativi omogenei e facilmente riconoscibili.

9. L'interoperabilità nei servizi della Pubblica amministrazione

Uno degli obiettivi principali del regolamento eIDAS 1.0 era quello di rafforzare l'interoperabilità dei servizi pubblici transfrontalieri all'interno dell'Unione europea. In particolare, la facilitazione dell'accesso ai servizi sanitari digitali è funzionale a sostenere la mobilità delle persone nello spazio europeo — studenti, lavoratori, turisti — e si inserisce nel più ampio quadro della strategia digitale dell'Unione. La sanità digitale rappresenta, in tale prospettiva, una componente centrale, in quanto strumentale alla piena realizzazione di diritti fondamentali quali la libertà di circolazione, l'accesso all'istruzione e la tutela della dignità umana.

Tuttavia, eIDAS 1.0 ha conseguito tale obiettivo soltanto in misura parziale, principalmente a causa dell'eccessiva frammentazione degli strumenti di identificazione elettronica e dei relativi assetti normativi a livello nazionale. Gli Stati membri hanno adottato modelli organizzativi eterogenei, riconducibili, in via generale, a tre tipologie: (i) sistemi nei quali l'amministrazione pubblica distribuisce direttamente ai cittadini gli strumenti di identificazione digitale; (ii) sistemi in cui l'autorità pubblica definisce standard qualitativi e cornice regolatoria, mentre l'erogazione dei servizi di identità è affidata a operatori di mercato; (iii) modelli nei quali il fornitore dell'identità digitale è interamente un soggetto privato.

Ne consegue che l'interoperabilità delle identità digitali risulta strettamente dipendente dalle regole nazionali, dall'organizzazione dei sistemi di identificazione fisica, dalle esigenze di sicurezza interna e dalle modalità con cui ciascuno Stato membro disciplina la distribuzione dell'identità digitale.

Esemplificativi sono i casi dell'Italia, dove l'accesso al Sistema Pubblico di Identità Digitale (SPID) richiede il possesso del codice fiscale; della Germania, che si fonda su un distinto numero di identificazione fiscale (TIN); e della

Francia, che utilizza il *Numéro d'inscription au Répertoire des Personnes Physiques* (NIRPP). Tali sistemi, strutturalmente differenti, costituiscono un rilevante ostacolo all'interoperabilità transfrontaliera e compromettono il funzionamento fluido delle applicazioni di *eGovernment* su scala europea.

L'introduzione dell'EUDI Wallet nell'ambito di eIDAS 2.0 (art. 5a) accresce significativamente il potenziale di una effettiva interoperabilità dei servizi pubblici transfrontalieri, consentendo agli individui di esercitare un più ampio potere di autodeterminazione nelle proprie interazioni sociali, culturali, sanitarie ed economiche.

Ulteriore tassello di tale strategia è rappresentato dall'Interoperable Europe Act, entrato in vigore nel gennaio 2025, che prevede l'obbligo di predisporre una valutazione di interoperabilità (art. 5) e di individuare soluzioni interoperabili europee ai sensi dell'art. 7, al fine di agevolare l'attuazione di requisiti vincolanti in materia. In questo quadro complessivo, l'interoperabilità sanitaria assume un ruolo centrale anche nella Dichiarazione europea sul Decennio digitale, in quanto elemento essenziale per garantire la libera circolazione delle persone, l'accesso ai servizi fondamentali e la più ampia realizzazione dei diritti nell'Unione.