CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Scientifico

IDENTITÀ DIGITALE SELETTIVA E PROTEZIONE DEI DATI PERSONALI: WALLET EUROPEO E RESPONSABILITÀ PER ATTRIBUTI ECCEDENTI

Il contributo analizza l'EUDI Wallet e l'IT-Wallet come infrastrutture della presenza giuridica della persona nell'ambiente digitale. La tesi è che il wallet non serva solo a identificare meglio, ma a identificare meno quando sia sufficiente provare un attributo. Da tale premessa deriva una ricostruzione della responsabilità dei soggetti pubblici e privati che richiedano o inducano la comunicazione di attributi eccedenti, in violazione dei principi di minimizzazione, proporzionalità e correttezza tra GDPR, eIDAS 2.0, Digital Services Act e diritto civile.

di **Antonio Visicchio**
IUS/01 - DIRITTO PRIVATO
Estratto dal n. 7/2026 - ISSN 2532-9871

Direttore responsabile
Alessio Giaquinto

Pubblicato, Giovedì 9 Luglio 2026

CamminoDiritto.it
ISSN 2532-9871

Abstract ENG

The article examines the EUDI Wallet and the Italian IT-Wallet as infrastructures of the legal presence of the person in the digital environment. Its thesis is that the wallet should not merely identify better, but identify less whenever proof of a single attribute is sufficient. On this basis, the article reconstructs the liability of public and private actors that request or induce the disclosure of excessive attributes, in breach of data minimisation, proportionality and fairness under the GDPR, eIDAS 2.0, the Digital Services Act and civil law.

1. Dalla protezione del dato alla misura dell'identità rivelata

Il diritto della protezione dei dati personali è stato spesso descritto come diritto del controllo: controllo sull'informazione che riguarda la persona, sulla sua circolazione, sulla sua conservazione e sul suo impiego. L'interessato vi appare come titolare di una serie di poteri (conoscere, accedere, rettificare, opporsi, cancellare) esercitati dinanzi a un apparato informativo che raccoglie e ordina dati personali. Questa figura non scompare. Ma non basta più. 1, 2, 3, 4, 5, 6

Nell'era digitale in cui oggi viviamo, il problema non è soltanto se un dato possa essere trattato. Infatti, non tutto ciò che identifica serve a qualificare; non tutto ciò che qualifica deve identificare. Vi sono situazioni nelle quali l'ordinamento, il mercato o l'amministrazione non hanno bisogno del nome, della data di nascita, dell'indirizzo, del documento, ma soltanto della prova di una qualità: la maggiore età, l'abilitazione professionale, la residenza, la titolarità di un permesso, l'appartenenza a una categoria giuridicamente rilevante.

Qui si consuma un passaggio teorico di notevole rilievo. La protezione non si esaurisce nel divieto o nel consenso. Essa si sposta a monte, nell'architettura stessa della rivelazione del dato. Non si tratta soltanto di dire sì o no al trattamento, ma di conformare la porzione

CamminoDiritto.it
ISSN 2532-9871

di identità che viene esposta nel rapporto digitale. Il consenso, da solo, non governa la misura; può anzi legittimare, nella pratica, forme di resa informativa quando il soggetto sia posto dinanzi all'alternativa tra comunicare più del necessario o restare escluso dal servizio.

Il portafoglio europeo di identità digitale si colloca esattamente in questa faglia. Esso promette di semplificare l'identificazione, ma la sua funzione più alta non è identificare sempre. È, piuttosto, consentire di non identificare quando l'identificazione piena è inutile, sproporzionata, eccedente. La tecnica, in questa prospettiva, non amplia soltanto la capacità dell'ordinamento di conoscere la persona; può anche limitarla, contenerla, misurarla.

Il lessico della minimizzazione acquista allora un significato nuovo. Non designa soltanto una regola di buona amministrazione del dato, né una clausola tecnica di compliance. Esprime una misura giuridica della presenza personale. Il soggetto non è più costretto a "consegnarsi" integralmente al servizio digitale. Può, d'altronde, apparire secondo attributi, e dunque secondo frammenti funzionali della propria identità.

La domanda privatistica nasce qui: chi decide quale attributo sia necessario? Chi risponde della richiesta eccedente? Quale rimedio spetta alla persona quando l'accesso a un servizio sia condizionato alla comunicazione di dati ulteriori rispetto a quelli pertinenti? E, soprattutto, può configurarsi una responsabilità da sovra-esposizione dell'identità digitale?

L'espressione può apparire nuova, ma il problema è antico. Ogni relazione giuridica implica una rappresentazione del soggetto. Il contraente, il consumatore, il paziente, il minore, il cittadino, l'utente non sono figure neutre: sono identità funzionali, ritagliate dalla norma secondo lo scopo del rapporto. Il digitale rende questa operazione più intensa e più rischiosa, perché ogni richiesta di attributo può trasformarsi in conservazione, correlazione, profilazione, circolazione ulteriore.

L'identità digitale selettiva, allora, non è una categoria informatica. È una categoria giuridica della misura. Essa impone di ripensare il rapporto tra persona, dato e responsabilità non più secondo la sola alternativa tra trattamento lecito e trattamento illecito, ma secondo il criterio, più sottile e più esigente, della proporzione tra qualità richiesta e fine perseguito.

2. Il portafoglio europeo di identità digitale nel Regolamento (UE) 2024/1183

CamminoDiritto.it
ISSN 2532-9871

Il Regolamento (UE) 2024/1183 modifica il Regolamento (UE) n. 910/2014 e istituisce il quadro europeo relativo all'identità digitale. La scelta dell'Unione non è marginale. L'identificazione elettronica non viene più considerata soltanto come infrastruttura di fiducia per le transazioni, ma come condizione di accesso ai servizi pubblici e privati in uno spazio digitale unitario. 7, 8

Il portafoglio europeo di identità digitale è destinato a consentire a persone fisiche e giuridiche di identificarsi, autenticarsi e condividere attestati elettronici di attributi in un contesto transfrontaliero. La novità non va ridotta a un mero avanzamento dell'identificazione elettronica. Se così fosse, il wallet sarebbe soltanto un documento più comodo, un contenitore digitale di credenziali già note, una tessera senza carta. Il suo significato sistematico è più profondo: l'identità non viene più pensata come blocco unitario, bensì come insieme di attributi giuridicamente spendibili. 9, 10

Il soggetto non è soltanto chi è; è anche ciò che può provare di essere rispetto a una determinata relazione. Questa scomposizione dell'identità in attributi non impoverisce la persona, se governata dal diritto; al contrario, può proteggerla. L'identificazione piena è spesso eccessiva. L'attributo selettivo è l'esatta quantità di persona richiesta dal rapporto.

La funzione del diritto è impedire che questa scomposizione degeneri in cattura. L'attributo, proprio perché più agevole da esibire, rischia di diventare più agevole da pretendere. Il pericolo non è soltanto il trattamento abusivo di un dato già acquisito, ma la normalizzazione della richiesta eccedente: chiedere tutto perché è tecnicamente possibile; pretendere più attributi perché il sistema li rende disponibili; subordinare l'accesso a un servizio alla rivelazione di una identità più ampia di quella necessaria.

In tal modo, la libertà promessa dal wallet potrebbe rovesciarsi nel suo contrario. Lo strumento nato per ridurre la frizione identificativa potrebbe diventare una infrastruttura di pressione identitaria. Di qui l'esigenza di spostare l'analisi dal titolare del wallet al soggetto che richiede l'attributo: la pubblica amministrazione, la piattaforma, il prestatore di servizi, il professionista, l'impresa, il wallet-relying party.

Il punto non è soltanto tecnico, ma civilistico. La richiesta di attributi è un atto inserito in una relazione. Può precedere un contratto, condizionare l'accesso a un servizio, incidere sulla libertà di scelta, determinare asimmetrie informative, selezionare utenti, escludere soggetti. Essa, dunque, deve essere valutata alla luce della correttezza, della buona fede, della proporzionalità e della tutela dell'affidamento.

La categoria del relying party, valorizzata anche dalla normativa di attuazione sulla registrazione dei soggetti che intendono fare affidamento sul wallet, conferma che la

CamminoDiritto.it
ISSN 2532-9871

richiesta di attributi non è un gesto neutrale. Essa è un comportamento qualificato, imputabile, tracciabile, suscettibile di controllo. Il diritto dell'identità digitale, perciò, non è soltanto diritto dell'emissione delle credenziali, ma anche diritto della domanda di identità. 11

3. IT-Wallet e diritto interno: l'art. 64-quater del Codice dell'amministrazione digitale

Nel diritto interno, il Sistema IT-Wallet trova la propria base nell'art. 64-quater del Codice dell'amministrazione digitale, introdotto nell'ambito delle misure di attuazione del PNRR. La disposizione istituisce il Sistema di portafoglio digitale italiano, destinato a valorizzare e rafforzare l'interoperabilità tra le banche dati pubbliche e a favorire la diffusione di servizi in rete erogati da soggetti pubblici e privati. 12, 13

La formula legislativa è significativa. Essa non guarda soltanto alla pubblica amministrazione, ma include l'interazione tra pubblico e privato. L'identità digitale diviene infrastruttura di accesso a servizi, rapporti, utilità. È, dunque, un dispositivo di circolazione giuridica della persona.

Tale circolazione deve essere sorvegliata. L'interoperabilità, se priva di limiti, può trasformarsi in esposizione sistemica. L'efficienza, quando si emancipa dalla proporzione, diventa dominio informativo. Il diritto privato è chiamato a intervenire proprio qui: non contro la tecnica, ma dentro la tecnica; non per arrestare il processo di digitalizzazione, ma per attribuirgli forma, responsabilità e misura.

Il parere reso dal Garante per la protezione dei dati personali sugli schemi di decreto relativi al Sistema IT-Wallet conferma la centralità della protezione dei dati già nella fase regolatoria. La consultazione preventiva dell'Autorità non è un adempimento ornamentale; è il segno che l'architettura del wallet non può essere valutata soltanto in termini di funzionalità amministrativa o di efficienza dei servizi, ma deve misurarsi con i rischi per gli interessati. 14

Il Sistema IT-Wallet, dunque, non può essere studiato solo come segmento del governo digitale. Esso si colloca in un punto di incrocio: amministrazione digitale, mercato dei servizi, protezione dei dati, identità personale, responsabilità civile. La persona vi entra non come utente astratto, ma come centro di imputazione di attributi, diritti, rischi e aspettative.

La dimensione nazionale assume, inoltre, un rilievo specifico perché il wallet italiano

CamminoDiritto.it
ISSN 2532-9871

potrà costituire la forma ordinaria di incontro tra cittadini, pubbliche amministrazioni e operatori privati. In tale contesto, il tema decisivo non sarà soltanto la disponibilità tecnica del servizio, ma la sua grammatica giuridica: quali attributi siano richiedibili, da chi, per quali finalità, con quali obblighi di informazione, con quali limiti di conservazione e con quali responsabilità in caso di eccesso.

La pubblica amministrazione digitale, se vuole restare amministrazione costituzionale, non può assumere la disponibilità del dato come equivalente della sua necessità. Il privato, se vuole operare in un ecosistema fiduciario, non può trasformare la credenziale in occasione di appropriazione informativa. La misura dell'identità diviene così un criterio comune di legalità amministrativa e di correttezza negoziale.

4. Minimizzazione, attributi e selective disclosure

Il principio di minimizzazione, enunciato dall'art. 5, par. 1, lett. c), GDPR, impone che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento. Nella pratica corrente, tale principio è stato spesso letto come regola interna al trattamento: raccogliere meno dati, conservarli per meno tempo, limitarne gli accessi, ridurne la circolazione. Questa lettura rimane corretta, ma non esaurisce la portata della norma. 15, 16, 17, 18, 19

Nel contesto dell'identità digitale selettiva, la minimizzazione opera prima della raccolta. Essa non governa soltanto ciò che accade dopo che il dato è stato acquisito; governa la legittimità stessa della domanda di identità. Se basta sapere che un soggetto è maggiorenne, chiedere la data di nascita è già troppo. Se basta provare una qualifica professionale, pretendere l'intero documento di identità può essere eccedente. Se basta accertare la residenza in un Comune, conservare indirizzo, codice fiscale e copia del documento può violare la misura funzionale del rapporto.

La selective disclosure, ossia la rivelazione selettiva degli attributi, traduce in architettura ciò che il GDPR prescrive in forma di principio. Essa consente al soggetto di comunicare soltanto l'informazione necessaria, lasciando non rivelato tutto ciò che non serve alla finalità. La protezione non nasce più soltanto dalla promessa del titolare del trattamento, ma dalla configurazione stessa del rapporto informativo.

Questo spostamento è decisivo. Il diritto della protezione dei dati ha conosciuto a lungo una tensione tra regole ex ante e rimedi ex post. Informative, consensi, registri, valutazioni d'impatto e misure di sicurezza appartengono al primo versante; reclami, sanzioni e risarcimenti al secondo. Il wallet, se correttamente progettato e utilizzato, può introdurre una terza forma di tutela: la prevenzione strutturale dell'eccedenza identitaria.

CamminoDiritto.it
ISSN 2532-9871

L'art. 25 GDPR consente di fondare giuridicamente tale passaggio. La protezione dei dati fin dalla progettazione e per impostazione predefinita non chiede soltanto di adottare misure tecniche adeguate. Essa impone che le impostazioni di default siano orientate alla limitazione del trattamento. Nel wallet, questa regola può assumere una forma molto concreta: l'opzione normale non deve essere la rivelazione dell'identità piena, ma la presentazione dell'attributo minimo idoneo a soddisfare la finalità. 20, 21

La tecnica, però, non basta. La selective disclosure protegge soltanto se il soggetto che richiede l'attributo è vincolato a chiedere il minimo. In caso contrario, il wallet offrirebbe all'utente la possibilità di rivelare meno, ma il servizio potrebbe continuare a pretendere di più. Il problema si sposta allora dal potere dell'interessato alla responsabilità del richiedente.

L'identità selettiva non è soltanto autodeterminazione informativa; è relazione regolata. Il diritto non deve limitarsi a celebrare la libertà dell'utente di scegliere quali attributi esibire, perché tale libertà è spesso debole, compressa da asimmetrie tecniche, economiche e sociali. Deve invece costruire doveri oggettivi di proporzione in capo a chi organizza il servizio e governa il punto di accesso.

5. Age assurance e tutela dei minori online tra GDPR e Digital Services Act

L'age assurance costituisce il caso applicativo più immediato dell'identità digitale selettiva. Essa non esaurisce il tema, ma lo rende visibile. Per impedire l'accesso dei minori a contenuti o servizi non appropriati, l'ordinamento non ha necessariamente bisogno di conoscere chi sia l'utente. Ha bisogno di sapere se egli superi una determinata soglia di età.

La differenza è essenziale. Un sistema che richieda copia del documento, data di nascita, nome, cognome, indirizzo o codice fiscale produce un'identificazione sovrabbondante rispetto allo scopo. Un sistema che consenta di provare soltanto il superamento della soglia di età realizza invece una tutela simultanea: protegge il minore dal contenuto nocivo e protegge l'adulto dalla rivelazione non necessaria della propria identità.

Il Digital Services Act, all'art. 28, impone ai fornitori di piattaforme online accessibili ai minori misure appropriate e proporzionate per garantire un elevato livello di privacy, sicurezza e protezione dei minori. La Commissione europea ha poi adottato linee guida dedicate alla protezione dei minori online, destinate a orientare la valutazione di conformità delle piattaforme. Il punto rilevante, ai fini del presente studio, è che la

CamminoDiritto.it
ISSN 2532-9871

protezione del minore non può essere realizzata sacrificando senza misura la protezione dei dati degli altri utenti. 22, 23

La stessa impostazione emerge dallo Statement 1/2025 dell'European Data Protection Board sull'age assurance. L'EDPB individua la necessità di soluzioni proporzionate, fondate sul rischio e rispettose dei principi di minimizzazione, protezione dei dati fin dalla progettazione e limitazione della finalità. L'età diviene così un attributo da provare, non una identità da consegnare. 24

Il diritto italiano offre un laboratorio significativo nella disciplina dell'accesso a contenuti pornografici online. L'art. 13-bis del d.l. n. 123/2023, convertito dalla l. n. 159/2023, vieta l'accesso dei minori a tali contenuti e affida all'AGCOM la definizione delle modalità tecniche e di processo per l'accertamento della maggiore età. La delibera AGCOM n. 96/25/CONS e il relativo Allegato A costruiscono un modello attento alla minimizzazione, alla separazione dei ruoli e al cosiddetto doppio anonimato. 25, 26

Tale modello è prezioso sul piano sistematico. Il sito o la piattaforma non dovrebbero conoscere l'identità dell'utente; il soggetto che fornisce la prova dell'età non dovrebbe conoscere il servizio al quale l'utente intende accedere. Si realizza così una doppia separazione informativa: chi conosce l'identità non conosce la destinazione; chi conosce la destinazione non conosce l'identità. Il diritto costruisce una distanza per impedire la cattura. 27

L'Age Verification Manual della Commissione europea, relativo all'EUDI Wallet, muove nella medesima direzione: il wallet consente di confermare il superamento di una soglia di età senza rivelare la data di nascita completa o altre informazioni identificative. Qui si coglie la forza della selective disclosure. Non è un artificio tecnico per specialisti, ma il modo in cui la protezione dei dati diventa forma del rapporto. 28

L'age assurance deve però restare, nel presente lavoro, un caso e non l'oggetto esclusivo dell'indagine. Se l'articolo si fermasse alla tutela dei minori, ricadrebbe in un campo già frequentato. Il punto più ampio è che ogni servizio digitale potrà essere tentato di chiedere più attributi del necessario: età, genere, residenza, qualifica, reddito, abilitazione, appartenenza, stato familiare, condizione sanitaria. L'age assurance mostra la strada; la responsabilità da sovra-esposizione ne definisce il presidio.

6. Relying parties e responsabilità da richiesta eccedente

La figura del wallet-relying party consente di individuare il punto giuridico della

CamminoDiritto.it
ISSN 2532-9871

responsabilità. Il relying party è il soggetto che richiede e utilizza l'informazione o l'attestato presentato mediante wallet. Non è un destinatario casuale del dato, ma il soggetto che formula la domanda di identità e organizza le condizioni di accesso al servizio.

Questa domanda non è neutrale. Essa può essere corretta o eccedente, proporzionata o invasiva, necessaria o meramente opportunistica. Può limitarsi a chiedere un attributo minimo, oppure può indurre l'utente a rivelare l'intera credenziale. Può essere costruita in modo chiaro, oppure mediante interfacce che spingano alla condivisione massima. Può rispettare la destinazione dell'attributo, oppure favorire conservazione, correlazione e riuso.

La normativa di attuazione sulla registrazione dei wallet-relying parties conferma che tale soggetto deve essere identificabile nel sistema. La registrazione non ha soltanto funzione amministrativa; essa rende possibile attribuire responsabilità a chi chiede attributi digitali. Il diritto della fiducia digitale non può restare diritto della sola infrastruttura: deve diventare anche diritto del comportamento del richiedente.

La responsabilità da richiesta eccedente può assumere forme diverse. In primo luogo, vi è la responsabilità da violazione dei principi del GDPR, quando la richiesta determini trattamento non conforme ai principi di minimizzazione, limitazione della finalità, trasparenza o protezione fin dalla progettazione. In secondo luogo, vi è la responsabilità da scorrettezza relazionale, quando l'accesso a un servizio sia subordinato a una comunicazione non necessaria di attributi e la posizione dell'utente sia compressa da asimmetria informativa o dipendenza funzionale. In terzo luogo, vi è la responsabilità da lesione della sfera personale, ove l'eccesso identitario produca danno risarcibile.

Nel rapporto contrattuale o precontrattuale, gli artt. 1175, 1337 e 1375 c.c. offrono clausole generali capaci di orientare il giudizio. La correttezza e la buona fede non impongono soltanto di non ingannare; impongono di non aggravare inutilmente la posizione dell'altra parte, di non pretendere informazioni eccedenti, di non abusare della propria posizione tecnica o organizzativa. La domanda di identità, se sproporzionata, può diventare una forma di abuso informativo. 29

Fuori dal rapporto obbligatorio, l'art. 2043 c.c. resta la clausola generale per la lesione ingiusta di interessi giuridicamente protetti. Tuttavia, occorre evitare scorciatoie. Non ogni richiesta eccessiva genera automaticamente un danno risarcibile. Il danno deve essere allegato e provato, secondo le regole proprie della fattispecie applicabile. Nel campo del GDPR, la Corte di giustizia ha chiarito che la mera violazione del regolamento non basta: occorrono violazione, danno e nesso causale, pur non essendo richiesto che il

CamminoDiritto.it
ISSN 2532-9871

danno non patrimoniale raggiunga una soglia minima di gravità. 30, 31, 32, 33, 34, 35, 36, 37, 38

Il rischio, dunque, è duplice: da un lato, banalizzare la responsabilità, trasformando ogni irregolarità in risarcimento; dall'altro, svuotarla, riducendo la sovra-esposizione a mera inosservanza formale. La via corretta è intermedia. La richiesta eccedente è giuridicamente rilevante già come violazione del modello di proporzione; diviene fonte di risarcimento quando produca un pregiudizio effettivo, anche non patrimoniale, causalmente collegato all'eccesso.

In questa prospettiva, la responsabilità del relying party non è responsabilità per il solo fatto di avere chiesto un dato. È responsabilità per avere chiesto più identità di quella che il rapporto richiedeva.

7. La sovra-esposizione dell'identità digitale come problema civilistico

La nozione di sovra-esposizione dell'identità digitale indica la comunicazione, la richiesta o l'induzione alla comunicazione di attributi personali eccedenti rispetto alla finalità del rapporto. Essa non coincide necessariamente con la divulgazione pubblica. Può realizzarsi anche in un rapporto riservato, quando il soggetto sia costretto a rendere conoscibili qualità o dati non necessari per ottenere un servizio, concludere un contratto, accedere a una piattaforma o interagire con la pubblica amministrazione.

La categoria deve essere tenuta distinta da figure vicine. Non è soltanto data breach, perché può avvenire senza violazione di sicurezza. Non è soltanto trattamento illecito, perché il problema può emergere già nella fase della richiesta. Non è soltanto lesione dell'identità personale classica, perché non riguarda necessariamente il travisamento dell'immagine sociale, ma l'eccesso di rivelazione funzionale. Non è soltanto profilazione, perché può precedere o rendere possibile la profilazione.

La sua peculiarità consiste nel rapporto tra finalità e identità. Il soggetto entra nella relazione con più persona di quanta ne occorra. L'ordinamento deve chiedersi se tale eccedenza sia giustificata. La domanda non è diversa, nella sua struttura, da quella che il diritto privato conosce quando misura la proporzione tra mezzo e scopo, tra potere e interesse, tra adempimento e aggravamento, tra informazione e affidamento.

L'identità personale, nella tradizione civilistica, è stata costruita come interesse alla corretta rappresentazione del soggetto. L'identità digitale selettiva impone un passaggio ulteriore: non soltanto essere rappresentati correttamente, ma non essere rappresentati più

CamminoDiritto.it
ISSN 2532-9871

del necessario. La persona non chiede solo di non essere deformata; chiede di non essere integralmente consegnata quando basta una qualità. 39, 40, 41, 42, 43, 44

In ciò risiede la portata privatistica della tesi. Il wallet non è soltanto una infrastruttura di sicurezza. È una tecnica di misura della personalità nel rapporto. La sua disciplina deve essere letta insieme alle categorie della persona, dell'affidamento, della correttezza e della responsabilità. La protezione dei dati personali diviene così diritto della misura, e il diritto privato torna a svolgere la sua funzione più propria: contenere il potere nella relazione.

La sovra-esposizione può produrre pregiudizi diversi. Può generare perdita di controllo informativo, rischio concreto di correlazione tra servizi, esclusione o discriminazione, esposizione indebita di qualità personali, incremento del rischio di frode o furto d'identità, compressione della libertà di scelta. La risarcibilità dipenderà dalla prova del danno e dal regime applicabile, ma la rilevanza dell'eccesso non può essere negata.

La recente letteratura tecnico-giuridica sui wallet digitali segnala, peraltro, un rischio empiricamente plausibile: gli utenti possono essere indotti a rivelare credenziali o attributi in misura superiore al necessario, soprattutto quando l'interfaccia o il contesto non offrono raccomandazioni chiare. Ciò conferma che la protezione non può essere affidata alla sola razionalità individuale dell'utente. Occorrono obblighi oggettivi di progettazione, richiesta minima e responsabilità del richiedente. 45

La categoria proposta non pretende di sostituire il GDPR, né di creare una responsabilità autonoma priva di base normativa. Essa mira a ordinare un fenomeno nuovo attraverso strumenti esistenti: minimizzazione, privacy by design, limitazione della finalità, correttezza, buona fede, affidamento, danno da trattamento illecito, illecito civile. Il suo valore è sistematico: mostra che l'identità digitale non è solo un problema di accesso, ma di misura giuridica della persona. 46, 47, 48, 49

8. Conclusioni: una teoria della proporzione identitaria

Il portafoglio europeo di identità digitale e il Sistema IT-Wallet italiano aprono una fase nuova nella disciplina della persona digitale. Il problema non è più soltanto garantire che l'identificazione sia sicura, interoperabile e transfrontaliera. Il problema è stabilire quanta identità debba circolare in ciascun rapporto.

La tesi qui proposta può essere riassunta in una formula: il wallet non tutela la persona perché consente di identificarla meglio, ma perché consente di identificarla meno. La sicurezza dell'identificazione resta essenziale, ma non esaurisce la funzione dello

CamminoDiritto.it
ISSN 2532-9871

strumento. La sua capacità più innovativa consiste nel rendere possibile una presenza selettiva: non il documento, ma l'attributo; non l'identità intera, ma la qualità necessaria; non la massima conoscenza, ma la conoscenza proporzionata.

Da questa prospettiva derivano tre conseguenze. La prima è che la minimizzazione deve essere letta come principio architetturale e relazionale. Essa non riguarda soltanto la fase successiva alla raccolta, ma la legittimità della richiesta di attributi. La seconda è che i relying parties assumono una posizione di responsabilità qualificata, perché governano la domanda di identità e possono trasformare il wallet in strumento di libertà o di pressione informativa. La terza è che la sovra-esposizione dell'identità digitale costituisce un problema civilistico, da ricostruire attraverso GDPR, eIDAS 2.0, DSA e clausole generali del diritto privato. 50

La disciplina europea dell'identità digitale non deve essere letta come pura normazione tecnica. Essa incide sul modo in cui la persona appare nel mercato, nell'amministrazione, nella piattaforma, nel contratto. Ogni attributo richiesto è una forma di qualificazione giuridica; ogni attributo eccedente è una possibile lesione della misura personale.

Il compito del giurista è impedire che la tecnica renda naturale ciò che giuridicamente resta eccezionale: chiedere più identità del necessario. La persona non è un fascio illimitato di dati disponibili. È un centro di imputazione che l'ordinamento deve proteggere anche nella forma minima, discreta, selettiva della sua apparizione digitale.

Per questo la futura stagione del wallet non si giocherà soltanto sull'efficienza delle credenziali, ma sulla qualità giuridica delle richieste. Un ecosistema digitale maturo non è quello in cui tutti possono identificare tutti, ma quello in cui ciascuno può chiedere e conoscere soltanto ciò che serve. La civiltà del dato, se vuole restare civiltà della persona, deve diventare civiltà della misura.

CamminoDiritto.it
ISSN 2532-9871

Note e riferimenti bibliografici

1. S.D. Warren, L.D. Brandeis, The Right to Privacy, in Harvard Law Review, 1890, p. 193 ss., riferimento storico da impiegare con misura, senza trasformare l'articolo in una ricostruzione genealogica della privacy.

2. Bundesverfassungsgericht, 15 dicembre 1983, Volkszählungsurteil, sul principio di autodeterminazione informativa nella società informatizzata.

3. S. Rodotà, Tecnologie e diritti, Bologna, il Mulino, 1995.

4. S. Rodotà, Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali, in Rivista critica del diritto privato, 1997, p. 583 ss.

5. S. Rodotà, Il diritto di avere diritti, Roma-Bari, Laterza, 2012.

6. Carta dei diritti fondamentali dell'Unione europea, artt. 7 e 8; CEDU, art. 8; Convenzione n. 108 del Consiglio d'Europa, come modernizzata dal Protocollo CETS n. 223.

7. Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

8. 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.

9. Sul portafoglio europeo di identità digitale, cfr. il nuovo art. 5-bis del Regolamento (UE) n. 910/2014, come modificato dal Regolamento (UE) 2024/1183; sul ruolo dei wallet-relying parties, cfr. il nuovo art. 5-ter e la normativa di esecuzione.

10. European Digital Identity Wallet Architecture and Reference Framework, versione aggiornata disponibile nel repository ufficiale dell'EU Digital Identity Wallet: documento tecnico-istituzionale non normativo, utile per definizioni, attori e interazioni dell'ecosistema wallet.

11. Commission Implementing Regulation (EU) 2025/848 of 6 May 2025, laying down rules for the application of Regulation (EU) No 910/2014 as regards the registration of wallet-relying parties.

12. D.lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, art. 64-quater, introdotto dall'art. 20 del d.l. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla l. 29 aprile 2024, n. 56.

13. Dipartimento per la trasformazione digitale, Sistema IT-Wallet, scheda istituzionale: il sistema è collegato all'introduzione dell'art. 64-quater CAD e alla costruzione del portafoglio digitale italiano.

14. Garante per la protezione dei dati personali, Parere sugli schemi di decreti del Presidente del Consiglio dei Ministri di cui all'art. 64-quater del d.lgs. 7 marzo 2005, n. 82, in tema di Sistema di portafoglio digitale italiano – Sistema IT-Wallet, provv. n. 469 del 4 agosto 2025, doc. web n. 10162651.

15. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, Regolamento generale sulla protezione dei dati personali.

16. F. Pizzetti, Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Torino, Giappichelli, 2016.

17. Art. 5, par. 1, lett. c), Regolamento (UE) 2016/679: principio di minimizzazione dei dati.

18. A.J. Biega, P. Potash, H. Daumé III, F. Diaz, M. Finck, Operationalizing the Legal Principle of Data Minimization for Personalization, in Proceedings of SIGIR 2020, p. 399 ss., per la dimensione tecnico-operativa della minimizzazione nei sistemi personalizzati.

19. A.J. Biega, M. Finck, Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems, 2021,

CamminoDiritto.it
ISSN 2532-9871

contributo tecnico-giuridico da utilizzare come supporto specialistico e non come fondamento normativo.

20. Art. 25 Regolamento (UE) 2016/679: protezione dei dati fin dalla progettazione e protezione per impostazione predefinita.

21. Art. 32 Regolamento (UE) 2016/679: sicurezza del trattamento; art. 35 Regolamento (UE) 2016/679: valutazione d'impatto sulla protezione dei dati.

22. Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali, in particolare art. 28 sulla protezione online dei minori.

23. Commissione europea, Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065, Comunicazione pubblicata nella Gazzetta ufficiale dell'Unione europea, 2025/C 5519.

24. European Data Protection Board, Statement 1/2025 on Age Assurance, adopted on 11 February 2025.

25. D.l. 15 settembre 2023, n. 123, convertito, con modificazioni, dalla l. 13 novembre 2023, n. 159, art. 13-bis, recante disposizioni per la verifica della maggiore età per l'accesso a siti pornografici.

26. AGCOM, delibera n. 96/25/CONS dell'8 aprile 2025, pubblicata il 12 maggio 2025, Adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159.

27. AGCOM, Allegato A alla delibera n. 96/25/CONS, ove sono indicati i requisiti minimi dei sistemi di verifica dell'età, tra cui minimizzazione, assenza di profilazione, doppio anonimato e separazione tra soggetto che fornisce la prova dell'età e servizio destinatario.

28. Commissione europea, The Age Verification Manual, EU Digital Identity Wallet, 2026: il caso d'uso della verifica dell'età viene collegato alla selective disclosure, con conferma della soglia di età senza rivelazione della data di nascita completa o di altri dati identificativi.

29. Nel diritto civile interno, il richiamo agli artt. 1175, 1337 e 1375 c.c. consente di leggere la richiesta eccedente di attributi come possibile violazione dei doveri di correttezza, buona fede e lealtà informativa.

30. L'art. 2043 c.c. resta clausola generale di responsabilità aquiliana per la lesione ingiusta di interessi giuridicamente protetti; l'uso dell'art. 2050 c.c. per attività digitali ad alto rischio è suggestivo ma, nel presente contributo, deliberatamente non assunto come fondamento principale, per evitare forzature non necessarie.

31. Art. 82 Regolamento (UE) 2016/679: diritto al risarcimento e responsabilità.

32. Corte di giustizia UE, 4 maggio 2023, C-300/21, UI c. Österreichische Post AG: la mera violazione del GDPR non basta a fondare il diritto al risarcimento; occorrono violazione, danno e nesso causale, senza soglia minima di gravità del danno non patrimoniale.

33. Corte di giustizia UE, 14 dicembre 2023, C-340/21, VB c. Natsionalna agentsia za prihodite: il timore di un possibile uso illecito dei dati può integrare danno non patrimoniale se concreto e fondato.

34. Corte di giustizia UE, 14 dicembre 2023, C-456/22, Gemeinde Ummendorf: da leggere in continuità con C-300/21 sul danno non patrimoniale da violazione del GDPR.

35. Corte di giustizia UE, 25 gennaio 2024, C-687/21, BL c. MediaMarktSaturn: l'errore umano nella consegna di un documento contenente dati personali non prova automaticamente l'inadeguatezza delle misure tecniche e organizzative; resta centrale l'accertamento concreto.

36. Corte di giustizia UE, 11 aprile 2024, C-741/21, GP c. juris GmbH: la funzione dell'art. 82 GDPR resta compensativa e non punitiva.

37. Corte di giustizia UE, 20 giugno 2024, C-590/22, PS c. PS GbR; Corte di giustizia UE, 20 giugno 2024, cause riunite C-182/22 e C-189/22, Scalable Capital GmbH, per gli sviluppi successivi sulla liquidazione del danno non patrimoniale ex art. 82 GDPR.

CamminoDiritto.it
ISSN 2532-9871

38. Cass., Sez. Un., 11 novembre 2008, nn. 26972-26975, sul danno non patrimoniale nel sistema interno: riferimento utile soltanto per il quadro civilistico generale e non per sostituire l'autonomia interpretativa dell'art. 82 GDPR.

39. Sulla nozione classica di identità personale, v. V. Zeno-Zencovich, Identità personale, in Digesto delle discipline privatistiche, sez. civ., vol. IX, Torino, UTET, 1993, p. 294 ss.

40. G. Resta, Identità personale e identità digitale, in Il diritto dell'informazione e dell'informatica, 2007, p. 511 ss.

41. G. Pino, Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale, Bologna, il Mulino, 2003.

42. G. Pino, L'identità personale, in S. Rodotà, P. Zatti, a cura di, Trattato di biodiritto. Ambito e fonti del biodiritto, Milano, Giuffrè, 2010.

43. G. Finocchiaro, Identità personale su Internet: il diritto alla contestualizzazione dell'informazione, in Il diritto dell'informazione e dell'informatica, 2012, fasc. 3.

44. Cass. civ., 22 giugno 1985, n. 3769, caso Veronesi, tradizionalmente richiamata tra i precedenti di riconoscimento del diritto all'identità personale; da usare solo se si amplia il paragrafo storico sulla formazione della categoria.

45. S. Zingg, D. Lain, Y. Nakatsuka, K. Kostiainen, S. Bechtold, S. Čapkun, Credential Disclosure in (EU) Digital Identity Wallets: Privacy Risks and Practical Mitigations, preprint 2026: fonte non peer reviewed, utile soltanto come indicatore empirico del rischio di eccessiva disclosure da parte degli utenti.

46. A. Mantelero, Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI, The Hague, T.M.C. Asser Press/Springer, 2022.

47. T.E. Frosini, O. Pollicino, E. Apa, M. Bassini, a cura di, Diritti e libertà in Internet, Milano, Le Monnier Università, 2017.

48. Il presente contributo assume la sovra-esposizione dell'identità digitale come categoria ricostruttiva, non come fattispecie autonoma tipizzata. La sua funzione è ordinare obblighi e rimedi già esistenti intorno alla proporzione tra attributo richiesto e finalità perseguita.

49. La distinzione tra illiceità del trattamento e danno risarcibile deve restare ferma: la prima può rilevare sul piano conformativo, inibitorio, sanzionatorio o rimediale; il secondo richiede allegazione e prova del pregiudizio, anche non patrimoniale, secondo il regime applicabile.

50. La responsabilità del relying party va intesa come responsabilità per eccesso nella domanda di identità: non per il solo fatto di richiedere un attributo, ma per l'assenza di necessità, proporzione e trasparenza nella sua richiesta o nel suo successivo impiego.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11839