RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0063
Articolo sottoposto a peer review

Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD

Alessandro Ortalda • Stefano Leucci

La proposta di emendamento al Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno ha rinvigorito il dibattito europeo sul tema dell'identità digitale. I vari problemi emersi da questo dibattito rendono necessario un miglior coordinamento della proposta con gli strumenti legislativi preesistenti. Il presente contributo mira ad analizzare i principali punti di frizione tra il quadro normativo legato alle identità elettroniche/digitali e la disciplina europea riguardante la protezione dei dati personali.

Identità elettronica – Identità digitale – eIDAS – RGPD

1. Introduzione

Il 23 luglio 2014, il Parlamento europeo ed il Consiglio hanno approvato il "Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno" (anche Regolamento 910/2014 o Regolamento eIDAS)[1]. A circa sette anni di distanza, il 3 giugno 2021, la Commissione europea ha presentato una proposta di emendamento al Regolamento eIDAS (anche eIDAS-2)[2], che introduce una serie di modifiche attualmente in fase di discussione. La proposta ha riportato l'attenzione su un argomento che, a livello europeo, sembrava aver perso visibilità rispetto ad altri aspetti legati al mondo digitale come la protezione dei dati personali e la sicurezza cibernetica.

Il rinnovato interesse per il tema dell'identificazione elettronica transfrontaliera coincide sia con una maggior attenzione a livello globale[3], sia con la strategia di governance digitale dell'Unione. Infatti, la crescita di valore degli asset digitali e dei servizi erogati attraverso Internet rappresenta un interessante ambito di sviluppo economico per l'Europa[4]. Tuttavia, la quasi totale egemonia delle grandi piattaforme extra europee può rappresentare un ostacolo per lo sviluppo di questo inespresso potenziale economico. In questo contesto, la creazione di un Mercato unico digitale europeo che permetta a cittadini e residenti autorizzati di accedere a servizi online in tutta Europa è un passaggio quasi obbligato, di cui l'identificazione elettronica transfrontaliera rappresenta un tassello fondamentale[5], come evidenziato dalla rela-

A. Ortalda è dottorando di ricerca presso la Vrije Universiteit Brussel; si occupa di identità digitale, protezione dei dati personali e cybersecurity. È inoltre responsabile delle attività di formazione presso il Brussels Privacy Hub. S. Leucci è responsabile legale e tecnologico presso il Garante europeo della protezione dei dati; le sue principali responsabilità riguardano la previsione strategica delle nuove tendenze tecnologiche, le questioni finanziarie e l'intelligenza artificiale. È fellow al Nexa Center for Internet & Society del Politecnico di Torino.

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

zione che accompagna la proposta di emendamento al regolamento eIDAS.

La modifica di uno strumento normativo comporta per sua stessa natura rischi che, se non adeguatamente indirizzati, possono manifestare impatti negativi per l'Unione e i suoi cittadini. Infatti, la proposta di emendamento del Regolamento eIDAS presenta alcuni aspetti potenzialmente problematici. Talvolta si tratta di problemi derivanti da nuove disposizioni introdotte nella proposta. Talvolta si tratta di problemi già presenti nel Regolamento eIDAS in vigore e rimasti invariati nella proposta di emendamento. Talvolta si tratta di potenziali problemi derivanti da possibili frizioni tra diritti degli individui e strumenti legati all'identificazione elettronica non adeguatamente indirizzati dagli strumenti normativi.

La proposta di emendamento è al vaglio di diversi organismi comunitari che dovranno esprimersi su eventuali modifiche[6]; pertanto, è verosimile ritenere che subirà ulteriori modifiche. Tuttavia, proprio in virtù della sua attuale modificabilità è importante sottolinearne gli aspetti problematici e fornire alle parti coinvolte spunti che possano aiutarle nel processo di miglioramento della proposta.

Specificamente, il presente contributo si propone di analizzare i principali punti di frizione tra il quadro normativo legato alle identità elettroniche/digitali[7] e la disciplina riguardante la protezione dei dati personali prevista dal *Regolamento generale sulla protezione dei dati* (anche RGPD)[8]. Il paragrafo 2 descrive i quadri normativi oggetto dell'analisi, rispettivamente quello delineato dal Regolamento eIDAS e dalla successiva proposta di emendamento e quello delineato dal RGPD. Il paragrafo 3 analizza i punti di frizione tra questi quadri normativi e le eventuali problematiche derivanti da tali punti di frizione, includendovi anche gli eventuali rischi di discriminazione che potrebbero derivare dall'utilizzo di sistemi di identificazione elettronica. Infatti, le nuove tecnologie hanno il potenziale di rivoluzionare i processi di identificazione a patto che mitighino adeguatamente i possibili problemi di discriminazione connessi al loro utilizzo e promuovano buone prassi legate alla protezione dei dati personali[9]. Il paragrafo 4, infine, presenta le conclusioni dell'analisi.

2. Presentazione del quadro normativo

2.1. Il governo delle identità digitali

In Europa, il Regolamento eIDAS rappresenta il principale strumento normativo riguardante il governo delle identità digitali. Il Regolamento eIDAS stabilisce un quadro normativo volto ad agevolare la creazione ed il governo di strumenti e processi comuni tra gli Stati membri dell'Unione europea per il riconoscimento transfrontaliero delle identità elettroniche per l'accesso a servizi digitali, istituendo, *inter alia*[10], le modalità di notifica e riconoscimento dei mezzi e regimi di identificazione elettronica. Per mezzi di identificazione elettronica, il Regolamento eIDAS intende «un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online»[11], mentre quando parla di regimi di identificazione elettronica intende «un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone giuridiche»[12].

Come indicato più sopra, il Regolamento eIDAS si occupa principalmente di definire l'ecosistema normativo per garantire l'interoperabilità tra i diversi mezzi e regimi di identificazione elettronica adottati nell'Unione. Non definisce dunque le modalità e finalità dei singoli regimi nazionali di identificazione elettronica – prerogativa che rimane dei singoli Stati membri – limitandosi ad indicare gli elementi minimi che tali regimi devono soddisfare per garantire l'interoperabilità con i regimi istituiti da altri Stati membri. Specificamente, il Regolamento eIDAS dispone le condizioni affinché i mezzi di comunicazione adottati dai diversi Stati membri possano venire reciprocamente riconosciuti[13] e dispone le modalità attraverso cui gli Stati membri notificano alla Commissione europea l'esistenza e le caratteristiche dei loro regimi di identificazione elettronica[14]. Si noti come il Regolamento eIDAS applichi le sue disposizioni solamente nel caso in cui «i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico»[15], escludendo pertanto i mezzi di identificazione utilizzati esclusivamente nell'ambito di servizi offerti da operatori privati. Il Regolamento eIDAS, altresì, non impone agli Stati membri l'obbligo di notificare un regime di identificazione elettronica, lasciando tale scelta alla discrezione dei singoli Stati membri.

Dalla pubblicazione del Regolamento eIDAS, avvenuta nel luglio del 2014, diversi elementi hanno contribuito a modificare lo scenario europeo ed internazionale, non ultimo l'emergenza del Covid-19. Questi hanno modificato le aspettative di utenti ed operatori di servizi in relazione alle caratteristiche che i regimi di identificazione elettronica devono soddisfare[16]. Inoltre, l'aspirazione di creare uno spazio europeo per le identità elettroniche appare disattesa dai bassi tassi di adozione di strumenti

transfrontalieri di identificazione elettronica[17]. Pertanto, la Commissione europea nel febbraio del 2020 sì è impegnata ad avviare un processo di revisione del Regolamento eIDAS con il duplice obiettivo di stimolare una maggiore adozione di strumenti di identificazione elettronica tra gli Stati membri e riscrivere un quadro normativo più adatto al mutato scenario[18]. Nel giugno 2021, la Commissione europea ha pubblicato una proposta contenente una lista di emendamenti al Regolamento eIDAS, due dei quali di particolare rilevanza.

La proposta di emendamento all'articolo 7 del Regolamento eIDAS modifica il processo di notifica e riconoscimento dei regimi di identificazione elettronica, introducendo l'obbligo per gli Stati membri di notificare un regime di identificazione elettronica entro 12 mesi dall'entrata in vigore del Regolamento. Nella proposta di emendamento, pertanto, la notifica cessa di essere una libera scelta degli Stati membri su base volontaria, diventando un requisito.

Con l'introduzione dell'articolo 6-*bis*, invece, la proposta di emendamento al Regolamento eIDAS introduce i cosiddetti "portafogli europei di identità digitale". Questi vengono definiti come «un prodotto e 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, conformemente all'articolo 6-*bis*, nonché per creare firme elettroniche qualificate e sigilli elettronici qualificati»[19]. Inoltre, al fine di «garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati transfrontalieri, ciascuno Stato membro emette un portafoglio europeo di identità digitale entro 12 mesi dall'entrata in vigore del presente regolamento»[20], rendendo i portafogli europei di identità digitale un elemento obbligatorio e fondamentale nel quadro normativo di eIDAS-2.

La modifica dell'articolo 7 e l'introduzione dell'articolo 6-*bis* denotano la volontà da parte della Commissione europea di intervenire con maggior decisione nel processo di creazione di uno spazio europeo per le identità elettroniche. I due emendamenti appaiono finalizzati rispettivamente a promuovere una maggiore adozione di strumenti di identificazione transfrontaliera tra gli Stati membri e a fornire ai cittadini e residenti autorizzati degli strumenti che garantiscano loro un maggior controllo sui propri dati personali, allontanandosi così dal paradigma dei sistemi di identificazione elettronica centralizzati[21]. A queste considerazioni si aggiunga tuttavia che, l'introduzione di un approccio di notifica obbligatoria in vece del precedente approccio volontario per gli Stati membri potrebbe inasprire ulteriormente i fattori di rischio, in quanto eventuali problematiche connesse al quadro normativo si manifesterebbero ovunque in Europa e non soltanto negli Stati membri che avessero deciso di partecipare allo spazio europeo di identificazione elettronica transfrontaliera. Pertanto, una analisi dei potenziali problemi risulta ancora più importante.

2.2. La protezione dei dati personali

Il principale strumento normativo europeo in materia di protezione dei dati personali è il Regolamento generale per la protezione dei dati personali. Emanato nel 2016 ed entrato in vigore nel 2018, il Regolamento abroga la precedente Direttiva 95/46/CE sulla protezione dei dati personali[22]. Il RGPD si applica ai trattamenti di dati personali che avvengono sul territorio dell'Unione europea, oppure nei casi in cui i trattamenti siano finalizzati ad offrire beni o servizi a cittadini europei, nonché nei casi in cui i trattamenti comportino il monitoraggio del comportamento di questi cittadini sul territorio dell'Unione europea. Il RGPD definisce dati personali «qualsiasi informazione riguardante una persona fisica identificata o identificabile»[23], mentre definisce trattamento «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»[24]. Da queste definizioni si evince già come l'utilizzo di strumenti di identità elettronica soddisfi, in moltissimi casi, i requisiti connessi ai trattamenti di dati personali, attivando pertanto l'applicabilità del RGPD.

La disciplina europea in materia di protezione dei dati personali si basa prevalentemente su principi fondanti[25]. L'applicazione di questi principi può variare, anche considerevolmente, a seconda del contesto. Pertanto, il RGPD è da intendersi come una norma di indirizzo che non può prescindere dalla valutazione caso per caso sulle migliori modalità di implementazione delle sue disposizioni. Per il principio di liceità, ogni trattamento di dati personali deve essere svolto sulla base del consenso del soggetto interessato dal trattamento (nel seguito, l'interessato) o di un'altra base legittima[26]. Connessi al principio di liceità vi sono i principi di correttezza e trasparenza[27]. Il primo prevede che le operazioni di trattamento non

siano eseguite in segreto e gli interessati siano adeguatamente informati dei potenziali rischi, oltreché prevedere che i titolari e responsabili del trattamento dei dati predispongano adeguate misure per conformarsi prontamente, per quanto possibile, alla volontà dell'interessato, specialmente quando il suo consenso costituisce la base giuridica del trattamento dei dati[28]. Il secondo si riferisce all'obbligo di adottare misure appropriate per tenere informati gli interessati riguardo gli utilizzi dei loro dati personali[29].

Il principio di limitazione della finalità[30] obbliga ad effettuare il trattamento di dati personali per una finalità specifica e ben definita e prevede che un trattamento possa essere esteso a scopi ulteriori solo nei casi in cui siano compatibili con la finalità iniziale[31]. Il trattamento dei dati per finalità non definite e/o illimitate è, pertanto, illecito.

Secondo il principio di minimizzazione dei dati[32], devono essere trattati solo i dati adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono raccolti e/o per le quali vengono successivamente trattati. Le categorie di dati scelte per il trattamento devono essere necessarie per conseguire l'obiettivo generale dichiarato delle operazioni di trattamento e la raccolta di dati deve essere limitata alle informazioni pertinenti per le finalità perseguite dal trattamento. Inoltre, secondo il principio di esattezza dei dati[33], devono essere adottate misure necessarie e ragionevoli per garantire che i dati siano esatti e mantenuti aggiornati.

Il principio di limitazione della conservazione[34] impone che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Pertanto, i dati devono essere cancellati o resi anonimi quando tali finalità siano state soddisfatte. A tal fine, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica, per garantire che i dati non siano conservati più a lungo del necessario[35].

Il principio di integrità e riservatezza dei dati[36] richiede che siano messe in atto misure tecniche o organizzative adeguate a proteggere i dati da accesso, uso, modifica, o divulgazione non autorizzati o da perdita, distruzione o danno accidentali. Il RGPD prevede che tali misure vengano attuate tenendo conto «dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche»[37].

Infine, il principio di responsabilizzazione (o, in inglese, *accountability*)[38] fornisce una cornice a tutti i precedenti. Secondo tale principio, l'organizzazione che tratta i dati personali deve essere competente nel trattare i dati in modo adeguato e deve essere in grado di comprovarlo[39]. L'essenza di questo principio è dunque quella di assicurarsi che vengano messe in atto misure che garantiscano il rispetto delle norme sulla protezione dei dati e di conservare le prove necessarie per dimostrarlo agli interessati e alle autorità di controllo. Il principio di responsabilizzazione estende la sua area non solo alla conformità delle attività di trattamento alle norme applicabili, ma anche all'efficacia delle misure[40].

Come anticipato, l'applicazione delle regole derivanti dai principi del RGPD deve essere valutata caso per caso e, pertanto, richiede una interpretazione flessibile. Tale flessibilità deve tenere in considerazione il contesto e i rischi per i diritti e le libertà dei soggetti interessati associati al trattamento. Proprio per indirizzare tali problematiche, il RGDP introduce la valutazione dell'impatto sulla protezione dei dati (DPIA), uno degli strumenti più importanti per la gestione del rischio. Il Gruppo di lavoro articolo 29 descrive la DPIA come «un processo per costruire e dimostrare la conformità»[41]. Tuttavia, qualificarlo come mero strumento di conformità potrebbe diminuirne i benefici in relazione ad una corretta protezione dei dati personali[42]. Questo risulta di particolare importanza in un contesto come quello dell'identità digitale, in cui le applicazioni di tali strumenti possono modificarsi nel tempo fino ad assumere modalità imprevedibili al momento iniziale dello sviluppo, così come discusso nel paragrafo 3.2.

3. Identità elettronica e rischi per gli individui

Recenti analisi hanno evidenziato come i punti di contatto tra il quadro normativo legato all'identificazione elettronica e quello legato alla protezione dei dati personali possano dare luogo a sovrapposizioni o frizioni in grado di rendere meno agevole l'implementazione di misure conformi[43]. Questo paragrafo si pone l'obiettivo di analizzare le principali problematiche derivanti dall'interazione tra il Regolamento eIDAS, compresa la sua proposta di emendamento, ed il RGPD. Risulta infatti chiaro come le norme sull'identificazione elettronica e quelle sulla protezione dei dati siano strettamente connesse tra di loro. Non soltanto in virtù del fatto che molte delle attività associate alla gestione e all'utilizzo di mezzi e regimi di identificazione elettronica possano qualificarsi come trattamenti di dati personali ai sensi del RGPD, ma anche per via dei riferimenti espliciti al RGPD

riportati sia dal Regolamento eIDAS che dalla sua proposta di emendamento.

Nell'impossibilità di procedere ad una trattazione sistematica di tutti i potenziali problemi legati all'applicazione del Regolamento eIDAS e della sua proposta di revisione[44], il presente contributo si focalizza su un sottoinsieme di problematiche, descrivendone le caratteristiche principali: la sovrapposizione tra il regime di responsabilità previsto da eIDAS e quello previsto dal RGPD; l'incompatibilità dell'insieme minimo di dati previsto da eIDAS con il principio della minimizzazione dei dati previsto dal RGPD; l'incompatibilità del requisito di ritirare il portafoglio europeo di identità digitale in caso di violazione o compromissione dello stesso con il principio di disponibilità dei dati previsto dal RGPD. Il paragrafo dedica anche spazio all'analisi di possibili rischi di discriminazione derivanti dall'utilizzo di soluzioni di identificazione elettronica, interrogandosi riguardo alle misure messe in campo da eIDAS per la minimizzazione di tali rischi.

3.1. Interazioni tra eIDAS e RGPD

3.1.1. Sovrapposizione tra il regime di responsabilità di eIDAS e del RGPD

L'articolo 11 del Regolamento eIDAS, non modificato dalla proposta di emendamento, definisce il regime di responsabilità da applicarsi in caso di transazioni elettroniche transfrontaliere. Si tratta di un sistema che punta a garantire la corretta attribuzione delle responsabilità tra le molte parti coinvolte nel contesto delle transazioni elettroniche transfrontaliere. Infatti, queste ultime sono caratterizzate da almeno tra passaggi, ognuno dei quali prevede il coinvolgimento di diverse parti: la creazione di una identità elettronica; la fornitura di mezzi di identificazione elettronica; l'autenticazione dell'utente.

Una identità elettronica viene creata sulla base dei dati di identificazione personale, ovverosia «un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica»[45]. Questo presuppone che, al fine di creare una identità elettronica valida, i dati del soggetto interessato vengano raccolti e registrati in maniera corretta. L'articolo 11.1 del Regolamento eIDAS attribuisce agli Stati membri la responsabilità dei danni causati per dolo o negligenza in fase di creazione dell'identità, in quanto gli Stati membri, al momento della creazione dell'identità elettronica all'interno dei loro regimi di identificazione elettronica, devono garantire «che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure [...] al momento in cui è rilasciata l'identificazione elettronica»[46]. Si pensi ad esempio ad un caso in cui i dati anagrafici di un individuo vengano registrati in maniera errata in fase di creazione dell'identità elettronica, causando l'impossibilità dello stesso di accedere a servizi offerti in un altro Stato membro. In tal caso, secondo la disciplina eIDAS, lo Stato membro che ha creato e rilasciato l'identità elettronica viene considerato responsabile del danno arrecato. Si noti come l'articolo 11.1 stabilisca esplicitamente che è lo Stato ad essere responsabile, attribuendogli la responsabilità anche nei casi in cui questo si affidi ad una terza parte per la creazione e rilascio delle identità elettroniche.

La fornitura e accesso ai mezzi di identificazione elettronica è condizione necessaria affinché gli utenti possano usufruire dei servizi di identificazione elettronica. L'articolo 11.2 del Regolamento eIDAS attribuisce la responsabilità per danni connessi ai mezzi di identificazione elettronica alla parte che rilascia suddetti mezzi. Si pensi ad esempio ad un caso in cui l'identità elettronica di un utente venga erroneamente associata ad un altro individuo, impedendo al legittimo proprietario di venire identificato nel corso di una transazione transfrontaliera. Si noti come l'articolo 11.2, a differenza dell'articolo 11.1, attribuisca la responsabilità in maniera generica alla parte coinvolta, senza nominare esplicitamente lo Stato membro. Questo significa che, qualora lo Stato membro abbia direttamente rilasciato i mezzi di identificazione elettronica, qualificandosi pertanto come "parte coinvolta", la responsabilità ricade sullo Stato membro stesso. Differentemente, qualora i mezzi di identificazione siano stati rilasciati da altre parti, la responsabilità potrebbe ricadere su queste ultime, ferme restando le ulteriori responsabilità previste dal sistema giuridico nazionale[47].

Infine, l'autenticazione dell'utente è il passaggio attraverso cui una identità elettronica viene utilizzata per accedere al servizio desiderato. Nel contesto di una autenticazione, il sistema verifica che l'identità elettronica abbia le caratteristiche adeguate o i permessi necessari affinché l'utente possa legittimamente accedere al servizio. L'articolo 11.3 del Regolamento eIDAS attribuisce la responsabilità per danni connessi alla procedura di autenticazione alla parte che gestisce suddetta procedura. Si pensi ad esempio ad un caso in cui un individuo non riesca ad accedere a dei sussidi pubblici a causa della mancata associazione alla sua identità elettronica delle autorizzazioni necessarie. Così come all'articolo 11.2, in questi casi la responsabilità è genericamente attribuita alla

parte responsabile, sia questa lo Stato membro o un fornitore di servizi.

Come si evince dalla descrizione di cui sopra, il Regolamento eIDAS definisce un regime di responsabilità ben preciso, associato a specifici momenti del ciclo di vita e di utilizzo di una identità elettronica. Differentemente, il RGPD prevede un regime di responsabilità caratterizzato da una minor compartimentalizzazione. Il RGPD sancisce che, qualora «più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano [...] responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato»[48]. Il problema deriva dal fatto che la divisione categorica applicata da eIDAS risulta impraticabile nel contesto di un trattamento di dati personali ai sensi del RGPD.

Anche dividendo un trattamento di dati personali in singoli elementi coerenti con i tre passaggi presentati da eIDAS (es., trattamento con finalità di creazione di una identità elettronica; trattamento con finalità di identificazione elettronica; trattamento con finalità di autenticazione elettronica), il regime di responsabilità di eIDAS risulta incompatibile con quello del RGPD qualora più parti siano coinvolte nel trattamento. Si consideri il già citato esempio di danni occorsi durante il processo di autenticazione e derivanti da un errata attribuzione di permessi. In tal caso, la situazione non risulta conforme né con il RGPD, in quanto il trattamento avviene in violazione del principio di esattezza dei dati[49], né con il Regolamento eIDAS. Tuttavia, qualora il trattamento veda il coinvolgimento di più titolari o responsabili del trattamento, l'attribuzione delle responsabilità verrebbe complicata da una difficile interpretazione. Infatti, laddove il RGPD prevede che la responsabilità venga attribuita a tutti i titolari e responsabili coinvolti, chiamati in solido a rispondere dei danni causati, nel Regolamento eIDAS la responsabilità ricade solo sulla «parte che gestisce la procedura di autenticazione»[50]. Non è chiaro se questa debba intendersi come una singola entità, il che renderebbe il regime di responsabilità incompatibile con quello previsto dal RGPD, o preveda la possibilità di attribuire la responsabilità a più entità, allineando i regimi di responsabilità del Regolamento eIDAS e RGPD.

Tuttavia, anche qualora si ammettesse una interpretazione che permetta di allineare le due norme, non è chiaro se, a seguito di una violazione prevista da entrambi gli strumenti normativi, questi si applichino indipendentemente l'uno dall'altro, se le violazioni possano in qualche modo essere assimilate, o se debba essere tenuta in considerazione una sola violazione prevedendo l'applicazione di uno solo dei regimi di responsabilità. Qualora l'interpretazione propenda per quest'ultimo scenario, risulta inoltre incerto quale dei due regimi debba essere applicato. Entrambi gli strumenti sono infatti regolamenti europei e appartengono alla stessa categoria delle fonti del diritto comunitario, rendendo incerto stabilire quale dei due strumenti debba prevalere. La decisione del legislatore di non attribuire esplicitamente al Regolamento eIDAS lo stato di *lex specialis* rispetto al quadro normativo sulla protezione dei dati personali[51] contribuisce a complicare il dilemma interpretativo.

3.1.2. Incompatibilità dell'insieme minimo di dati con il principio della minimizzazione dei dati

Uno dei requisiti minimi richiesti dalla normativa per garantire l'interoperabilità tra i differenti regimi di identificazione elettronica degli Stati membri è quello di associare ad ogni identità elettronica un insieme minimo di dati di identificazione. Questo insieme viene dettagliato nel *Regolamento di esecuzione 2015/1501* della Commissione relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno [nel seguito, Regolamento di esecuzione eIDAS]. Come dettagliato nell'allegato al Regolamento di esecuzione eIDAS, questo insieme minimo di dati include il nome e cognome attuali dell'individuo, la sua data di nascita ed un identificativo univoco. Durante una transazione, questi dati vengono trasmessi tra le parti coinvolte per garantire l'autenticità dell'identità elettronica.

L'esistenza di un insieme minimo e obbligatorio di dati personali da associare alle identità elettroniche si pone direttamente in contrasto con il principio della minimizzazione dei dati sancito dal RGPD[52], che stabilisce che i dati oggetto di un trattamento debbano essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Non è difficile immaginare servizi che richiedano un numero di informazioni più limitato rispetto a quelle dell'insieme minimo di dati (basti pensare a servizi che richiedono solamente la verifica della maggiore età, senza necessità di conoscere l'esatta data di nascita dell'individuo).

Il tema della coerenza di eIDAS con il principio di minimizzazione dei dati è noto da tempo alla comuni-

tà accademica[53]. La stessa Commissione europea nel suo rapporto sulla valutazione degli impatti del Regolamento eIDAS menziona questo problema[54]. La proposta di emendamento al Regolamento eIDAS ha accolto queste osservazioni, introducendo alcune modifiche specifiche. Pur non abolendo l'insieme minimo di dati, la proposta di emendamento chiarisce che il «portafoglio europeo di identità digitale dovrebbe consentire, a livello tecnico, la divulgazione selettiva degli attributi alle parti facenti affidamento sulla certificazione [...], rafforzando in tal modo la praticità e la tutela dei dati personali, compresa la minimizzazione del trattamento di questi ultimi»[55]. Nonostante il Garante europeo della protezione dei dati abbia accolto con favore la scelta della proposta di emendamento[56], la decisione di limitare questo elemento ad un considerando, senza dedicare specifici articoli all'interno della norma, oltre al linguaggio utilizzato, aperto ad una interpretazione che lascia spazio di manovra ("dovrebbe consentire"), indebolisce la salvaguardia dei diritti degli interessati.

3.1.3. Disponibilità dei dati in caso di ritiro del portafoglio europeo di identità digitale

L'articolo 10-*bis* della proposta di emendamento al Regolamento eIDAS regola la sospensione, revoca o ritiro dei portafogli europei di identità digitali in caso di violazione o compromissione che possano pregiudicarne l'affidabilità o l'affidabilità di altri portafogli europei di identità. L'articolo prevede che a seguito di violazione o compromissione, lo Stato membro sospenda l'emissione e revochi la validità del portafoglio. Qualora non venga posto rimedio alla violazione o compromissione entro tre mesi, o qualora la violazione o compromissione risulti di particolare gravità, lo Stato membro ritira il portafoglio e comunica il ritiro agli altri Stati membri. L'articolo 10-*bis* della proposta di emendamento affianca e non sostituisce l'articolo 10 del Regolamento eIDAS, che sancisce simili disposizioni nel contesto di violazioni o compromissioni dei regimi di identificazione elettronica.

Come si evince sia dall'articolo 10-*bis* della proposta di emendamento che dall'articolo 10 del Regolamento eIDAS, sono previste tre misure a contenimento dei rischi. La sospensione dell'emissione del portafoglio o del regime di identificazione, la revoca della validità del portafoglio o del regime di identificazione ed il ritiro del portafoglio o del regime di identificazione. Il significato dei termini sospensione, revoca e ritiro in relazione ad una violazione o compromissione non viene precisato né dal Regolamento eIDAS né dalla proposta di emendamento. Il Regolamento eIDAS fornisce ulteriori elementi, precisando la distinzione tra il termina sospensione e revoca in relazione ai certificati qualificati, indicando che la «sospensione dei certificati qualificati è [...] diversa dalla revoca e comporta la perdita di validità temporanea di un certificato»[57]. Per estensione, è pertanto possibile affermare che quanto definito per i certificati qualificati possa essere applicato anche ai regimi di identificazione elettronica e ai portafogli europei di identità digitale implicando che, almeno per quanto riguarda la sospensione, la misura sia da intendersi come limitata nel tempo.

Il testo della norma non definisce i termini emissione e validità, che sono dunque da intendersi nel loro significato proprio. La Tabella 1 ricostruisce le diverse casistiche previste dal Regolamento eIDAS e dalla proposta di emendamento e propone una chiave interpretativa.

Come si evince dall'articolo 10 del Regolamento eIDAS e dall'articolo 10-*bis* della proposta di emendamento, è possibile identificare quattro casistiche che potrebbero configurare una impossibilità da parte degli utenti di accedere ai propri dati personali: in caso di revoca del regime di identificazione elettronica, di ritiro del regime di identificazione elettronica, di revoca della validità del portafoglio europeo di identità elettronica e di ritiro del portafoglio europeo di identità elettronica. Le due casistiche legate alla sospensione, invece, appaiono potenzialmente esenti in quanto, interrompendo il servizio solo in relazione a futuri utenti per i quali non sia ancora stato avviato alcun trattamento di dati personali, non configurerebbero alcuna violazione delle norme sulla protezione dei dati personali.

Negli altri casi, invece, l'impossibilità di accedere ai propri dati personali potrebbe configurarsi come una violazione del RGPD, che sancisce che debbano essere implementate misure che garantiscano la disponibilità dei sistemi e dei servizi[58]. Ovviamente, la necessità di tenere conto dei rischi per i diritti e le libertà delle persone fisiche non esclude a priori che la revoca o ritiro di suddetti strumenti possa essere compiuta in conformità al quadro normativo. Il titolare del trattamento è chiamato a svolgere una DPIA relativamente ai rischi derivanti dalla violazione o compromissione ed ai rischi derivanti dall'impossibilità per gli utenti di accedere ai proprio dati. Sulla base di tale valutazione dei rischi, il titolare determina le azioni da mettere in atto. Tuttavia, alcuni elementi concorrono a modificare le considerazioni sul rischio del titolare. Il primo concerne la tempestività di azione del titolare. Sia l'articolo 10 del Regolamento eIDAS che l'articolo 10-*bis* della proposta di emendamento prevedono che la revoca di, rispettivamente, regimi di identificazione elettro-

Strumento	*Articolo*	*Casistica*	*Durata*	*Proposta di interpretazione*
Regolamento eIDAS	Articolo 10	Sospensione del regime di identificazione elettronica	Temporanea	Interruzione temporanea nella distribuzione di nuove utenze associate al regime di identificazione elettronica
Regolamento eIDAS	Articolo 10	Revoca del regime di identificazione elettronica	Non specificata dalla norma	Interruzione del funzionamento del regime di identificazione elettronica
Regolamento eIDAS	Articolo 10	Ritiro del regime di identificazione elettronica	Non specificata dalla norma	Rimozione del regime di identificazione elettronica dalle liste notificate agli Stati membri
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Sospensione dell'emissione del portafoglio europeo di identità elettronica	Temporanea	Interruzione temporanea nella distribuzione di nuovi portafogli europei di identità elettronica all'utenza
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Revoca della validità del portafoglio europeo di identità elettronica	Non specificata dalla norma	Interruzione del funzionamento dei portafogli europei di identità elettronica
Proposta di emendamento al Regolamento eIDAS	Articolo 10-*bis*	Ritiro del portafoglio europeo di identità elettronica	Non specificata dalla norma	Rimozione dei portafogli europei di identità elettronica dalle liste notificate agli Stati membri

Tabella 1: Misure da adottarsi a seguito di violazione o compromissione e relativa proposta di interpretazione

nica e portafogli europei di identità digitale avvenga senza indugio in caso di violazione o compromissione. L'articolo 10-*bis* prevede anche che, in caso di violazione o compromissione di particolare gravità, il ritiro dei portafogli avvenga senza indugio. Questi elementi aggiungono fattori di rischio per i diritti e le libertà delle persone fisiche, in quanto non fornirebbero all'utente il tempo necessario a poter trasferire i suoi dati presso un altro regime o portafoglio. Inoltre, la mancata qualificazione di cosa costituirebbe una violazione o compromissione di particolare gravità ai sensi dell'articolo 10-*bis* della proposta di emendamento impone alle parti coinvolte di dover decidere autonomamente, senza possibilità di consultare organismi di supporto (quali, ad esempio, team nazionali di risposta incidenti informatici, autorità garanti per la privacy, etc.). Infatti, le disposizioni non forniscono alle parti coinvolte un orizzonte temporale sufficiente per svolgere attività di verifica dell'effettiva criticità della violazione o compromissione.

Il secondo elemento da tenere in considerazione durante l'analisi dei rischi è la durata prevista per le misure di mitigazione. Infatti, una misura temporanea pone minori rischi per i diritti e le libertà delle persone fisiche rispetto a una misura permanente. La mancata definizione della durata o, almeno, dell'indicazione se si tratti di misure temporanee o permanenti comporta una ulteriore difficoltà per il titolare del trattamento chiamato a svolgere una analisi dei rischi. Questa complessità è parzialmente indirizzata dalla *Decisione di esecuzione 2015/1984* della Commissione che definisce le circostanze, i formati e le procedure della notifica di cui all'articolo 9, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno [nel seguito, Decisione di esecuzione eIDAS]. Questo prevede che all'atto di notifica di un regime di identificazione elettronica da parte di uno Stato membro, quest'ultimo descriva «le disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra»[59]. Il Regolamento eIDAS lascia dunque libertà agli Stati membri di dettagliare quanto concerne la sospensione e la revoca dei regimi di identificazione elettronica, creando ulteriore confusione.

La proposta di emendamento del Regolamento eIDAS dovrebbe introdurre modifiche volte a chiarire il quadro normativo in relazione ai punti di cui sopra. In particolare, dovrebbe specificare il significato dei termini utilizzati, precisando gli orizzonti temporali assegnati ad ognuno di questi, dovrebbe fornire ulteriori indicazioni sui parametri da valutare per stabilire la criticità di una violazione o compromissione. Inoltre, dovrebbe uniformare le disposizioni legate alla sospensione, revoca e ritiro dei regimi di identità elettronica e dei portafogli europei di identità digitali, rimuovendo tale decisione dalle prerogative degli Stati membri o, almeno, identificando dei parametri minimi che questi devono rispettare.

Inoltre, sarebbe opportuno che il regime eIDAS prevedesse delle soluzioni di continuità in caso di sospensione, revoca o ritiro. Ad esempio, potrebbe introdurre un regime di trasferimento automatico dei dati di un utente presso un diverso regime o portafoglio. Questo potrebbe prevedere un trasferimento nazionale qualora uno Stato membro abbia notificato più di un regime di identificazione elettronica o più di un portafoglio europeo di identità digitale, o un trasferimento transfrontaliero, qualora non vi siano altre soluzioni presenti sul territorio dello Stato membro. In quest'ultimo caso, eIDAS dovrebbe definire un quadro uniforme per la stipula di accordi tra Stati membri finalizzati specificamente a questa evenienza.

3.2. eIDAS e rischi di discriminazione

I rischi legati alla discriminazione derivano dal ruolo di primaria importanza che i sistemi di identificazione elettronica possono ricoprire nelle vite degli individui. Come dimostrato dalle vicende giudiziarie di paesi extra europei, si tratta di problemi tangibili che possono manifestarsi in relazione a problemi tecnici o procedurali, sistematizzare situazioni di discriminazione precedentemente esistenti, o esacerbare situazioni di discriminazione nei confronti degli individui più vulnerabili[60]. Una discriminazione si materializza concretamente nel momento in cui ad un individuo viene impedito di esercitare un diritto, come ad esempio la negazione di accesso ad un servizio pubblico. La disciplina europea in materia di identificazione elettronica risulta pertanto direttamente impattata da questo tema, in quanto stabilisce la modalità per garantire l'accesso transfrontaliero a servizi elettronici da parte dei cittadini. Inoltre, il problema risulta ancora più importante in virtù della strategia di armonizzazione dei sistemi digitali prevista dal *Regolamento (UE) 2018/1724* del Parlamento europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012 (nel seguito, Regolamento 2018/1724). Infatti, eventuali problematiche che dovessero portare a situazioni di discriminazione potrebbero risultare amplificate a seguito delle disposizioni del Regolamento 2018/1724, aumentando gli impatti per i diritti e le libertà degli individui. Il problema è emerso anche in ambito extra europeo. Il giudizio *Aadhaar* della Corte suprema indiana ha stabilito che l'esclusione di un individuo dai benefici e dai sussidi a cui avrebbe diritto è una violazione della sua dignità e dunque conduce ad una discriminazione[61]. Il giudizio indiano afferma anche che nonostante l'efficienza sia un elemento fondamentale dell'operato della pubblica amministrazione, non può essere considerata come una giustificazione per compromettere la dignità dell'individuo. Dunque, un sistema di identità digitale deve tendere all'inclusività più ampia possibile.

Per quanto riguarda il Regolamento eIDAS e la proposta di revisione, se da un lato il Regolatore europeo si dimostra attento ai problemi che possono affliggere persone soggette da disabilità, introducendo specifiche disposizioni sia nel Regolamento eIDAS[62] che nella proposta di revisione[63], dall'altro entrambi gli strumenti si rivelano carenti nell'istituire misure a salvaguardia degli individui dai rischi di discriminazione. Si consideri, ad esempio, il tema dell'alfabetizzazione digitale. Secondo il *Digital Economy and Society Index* (indicatore sulla economia e società digitale) 2021, il 13% della popolazione europea non possiederebbe alcuna competenza digitale, mente solo il 56% della popolazione possiederebbe livelli base di alfabetizzazione digitale[64]. Per quanto semplici possano venire progettati e realizzati, gli strumenti di identificazione elettronica, richiederanno sempre un certo livello di alfabetizzazione digitale. Anche ammettendo che tutta la fascia di popolazione a bassa alfabetizzazione sia in grado di utilizzare tali strumenti in maniera adeguata, il 13% senza alcuna alfabetizzazione – che corrisponde a più di 58 milioni di persone all'interno dell'Unione[65] – rimarrebbe escluso dalla possibilità di utilizzare tali strumenti. Pertanto, la scelta di non considerare questo punto all'interno del Regolamento eIDAS o della sua proposta di revisione appare problematico, visto il numero di individui potenzialmente impattato.

La normativa dovrebbe prevedere almeno l'esecuzione obbligatoria di una valutazione di impatto. Infatti, seppure sia possibile affermare che le casistiche ricomprese dal perimetro normativo del Regolamento eIDAS e della sua proposta di revisione soddisfino i requisiti minimi per attivare l'obbligo di svolgere una DPIA, rimane comunque un margine di discrezionalità che potrebbe comportare dei rischi residuali per gli individui.

4. Conclusione

Allo stato attuale, il quadro normativo legato all'identificazione elettronica presenta alcune problematiche derivanti dall'interazione con le norme riguardanti la protezione dei dati personali e dalla mancata considerazione di problemi legati alla discriminazione degli individui. Specificamente, il presente contributo analizza quattro di questi problemi. Il primo riguarda la sovrapposizione tra regimi di responsabilità previsti dal Regolamento eIDAS e dalla sua propo-

sta di revisione con quello previsto dal RGPD. Tale sovrapposizione rende più complessa l'identificazione dei ruoli delle parti coinvolte e l'attribuzione delle relative responsabilità. Il secondo deriva dall'incompatibilità tra l'esistenza di un insieme minimo di dati previsto per le identificazioni elettroniche e il principio di minimizzazione dei dati sancito dal RGPD. Il terzo riguarda i potenziali rischi di non conformità con il principio di disponibilità dei dati sancito dal RGPD di alcune azioni mitigative previste dal Regolamento eIDAS e dalla sua proposta di emendamento da attuarsi a seguito di compromissione o violazione degli strumenti di identificazione previsti da tali norme. Il quarto ed ultimo problema riguarda la mancanza di misure per indirizzare eventuali rischi di discriminazione connessi all'implementazione di misure di identificazione elettronica.

Pur presentando tali problemi, il quadro normativo non risulta compromesso. Nessuno dei problemi analizzati appare infatti bloccante e le incertezze interpretative possono essere risolte attraverso una maggior chiarezza del testo della norma. In tal senso il processo di revisione di eIDAS avviato dalla Commissione europea rappresenta l'opportunità per affrontare questi problemi e definire un nuovo quadro normativo più in linea con il RGPD e gli altri strumenti normativi comunitari.

Note

[1] European Commission, *Commission proposes a trusted and secure Digital Identity for all Europeans*, 3 June 2021.

[2] *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 2021*, COM(2021) 281 final del 3 giugno 2021.

[3] Si veda, a titolo di esempio, la bozza di risoluzione delle Nazioni Unite sul riconoscimento dei sistemi di identità nelle transazioni transfrontaliere. United Nations, *Draft Provisions on the Use and Cross-border Recognition of Identity Management and Trust Services 2021*, 26 January 2021.

[4] Si veda Oxford Economics, *Digital Services in Europe. An Evidence Review*, 2020.

[5] A questo si aggiungano altri strumenti legislativi attualmente in fase di definizione quali, ad esempio, la legge sui servizi digitali. Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE 2020*, COM(2020) 825 final del 27 aprile 2021.

[6] Per informazioni relative all'attuale stato di lavorazione della proposta presso le istituzioni comunitarie si veda European Parliament - Legislative Observatory, *European Digital Identity Framework. 2021/0136(COD)*.

[7] Ai fini del presente contributo, i termini "elettronico" e "digitale" sono considerati sinonimi.

[8] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*.

[9] A. Beduschi, *Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights*, in "Big Data & Society", July 2019.

[10] Oltre agli strumenti di identità digitale descritti dal presente contributo, il Regolamento eIDAS istituisce e regola svariati istituti utili ai servizi fiduciari elettronici nel Mercato unico digitale europeo.

[11] *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 e che abroga la direttiva 1999/93/CE (910/2014)*, art. 3.2.

[12] *Ivi*, art. 3.4.

[13] *Ivi*, art. 6.

[14] *Ivi*, art. 9.

[15] *Ivi*, art. 7.b.

[16] European Commission, *Commission Staff Working Document. Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) N. 910/2014 as Regards Establishing a Framework for a European Digital Identity*, 3 June 2021.

[17] Il rapporto sugli impatti del Regolamento eIDAS pubblicato dalla Commissione europea lamenta, alla data di pubblicazione, un tasso di adozione del 59%.

[18] European Commission, *Shaping Europe's Digital Future*, February 2020.

[19] COM(2021) 281 final, cit., art. 3.42.

[20] *Ivi*, art. 6-*bis*.1.

[21] Si veda ad esempio C. Allen, *The Path to Self-Sovereign Identity*, in "Life With Alacrity", 25 April 2016.

[22] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati 1995 (95/46/CE)*.

[23] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, art. 4.1. Si noti che, come espresso dal Gruppo di lavoro articolo 29 per la protezione dei dati, il concetto di dato personale è da intendersi in maniera ampia e dinamica, piuttosto che come un insieme prestabilito di informazioni fisso nel tempo. Si veda Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 04/2007 sul concetto di dati personali*, giugno 2007.

[24] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 4.2.

[25] *Ivi*, art. 5.

[26] Oltre al consenso, il RGPD prevede cinque presupposti legittimi per il trattamento dei dati, e cioè quando il trattamento dei dati personali sia necessario per l'esecuzione di un contratto, per l'esecuzione di un compito connesso all'esercizio di pubblici poteri, per adempiere un obbligo legale, per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, o se necessario per la salvaguardia degli interessi vitali dell'interessato. *Ivi*, art. 6.1.

[27] *Ivi*, art. 5.1.a.

[28] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on Data Protection Law*, 2018, p. 133.

[29] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 12.

[30] *Ivi*, art. 5.1.b.

[31] Gruppo di lavoro articolo 29 per la protezione dei dati, *Parere 03/2013 sulla limitazione delle finalità*, 2 aprile 2013.

[32] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.1.c.
[33] *Ivi*, art. 5.1.d.
[34] *Ivi*, art. 5.1.e.
[35] CEDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008, 3052/04, 30565/04.
[36] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.1.f.
[37] *Ivi*, art. 32.
[38] *Ivi*, art. 5.2.
[39] *Ibidem*.
[40] *Ivi*, considerando 74.
[41] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679*, 4 aprile 2017, p. 13.
[42] Si veda R. Gellert, *Understanding the Notion of Risk in the General Data Protection Regulation*, in "Computer Law & Security Review", vol. 34, 2018, n. 2, p. 279-288. Si veda anche J. Van Rest, R. Sanchez-Reillo, G. Whittaker et al., *Technical and Operational Issues Associated with Early Warning Zones for Critical Infrastructure*, Publications Office of the European Union, 2019, p. 109.
[43] Si veda a titolo di esempio A. Ortalda, N. Tsakalakis, L. Jasmontaite, *The European Commission Proposal Amending the eIDAS Regulation (EU) No 910/2014: A Personal Data Protection Perspective*, Brussels Privacy Hub, 24 December 2021, p. 5.
[44] Si vedano, a titolo di esempio, European Data Protection Supervisor, *Formal Comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity*, 28 July 2021; Comitato europeo delle Regioni, *Opinione: Identità digitale europea (2022/C 61/09)*, 21 ottobre 2021; Comitato economico e sociale, *e-ID (identificazione elettronica) (INT/951-EESC-2021)*, 20 ottobre 2021.
[45] AGID, *Regolamento eIDAS*, art. 3.3.
[46] *Ivi*, art. 7.d.
[47] *Ivi*, artt. 11.4, 11.5.
[48] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 82.4.
[49] *Ivi*, art. 5.d.
[50] AGID, *Regolamento eIDAS*, cit., art. 11.3.
[51] Soluzione che, al contrario, è stata applicata in altri strumenti europei. Si veda *Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) 2002 (2002/56/CE)*, art. 1.
[52] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 5.c.
[53] Si veda N. Tsakalakis, S. Stalla-Bourdillon, K. O'hara, *Data Protection by Design for Cross-Border Electronic Identification: Does the EIDAS Interoperability Framework Need to Be Modernised?* in E. Kosta, J. Pierson, D. Slamanig et al. (eds.), "Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", Springer, 2019.
[54] European Commission, *Commission Staff Working Document. Impact Assessment Report*, cit. «While eIDAS notified eIDs offer a high level of security, it has limitations as regards the principle of data minimisation. For authentication to online public services cross-border, it is compulsory to exchange the full minimum eIDAS data set and there is no possibility for the user to limit the transmitted personal data to the minimum required for a specific transaction».
[55] COM(2021) 281 final, cit., considerando 29.
[56] European Data Protection Supervisor, *Formal Comments of the EDPS*, cit. «The EDPS welcomes that the European Digital Identity Wallet will give the user better and transparent control on what data to share with whom for what purposes. The technical solution envisaged would be able to solve problems of excessive data processing, as it would allow the data subject to actually reveal only those data that are necessary for a specific purpose».
[57] AGID, *Regolamento eIDAS*, cit., considerando 53.
[58] Garante per la protezione dei dati personali, *Regolamento generale sulla protezione dei dati*, cit., art. 32.1.
[59] Commissione europea, *Decisione di esecuzione 2015/1984 della Commissione che definisce le circostanze, i formati e le procedure della notifica di cui all'articolo 9, paragrafo 5, del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, 3 novembre 2015, art. 4.1.3.
[60] Si veda *A Guide to Litigating Identity Systems*, in "Privacy International", 15 September 2020.
[61] Si veda Supreme Court of India, *Justice K.S. Puttaswamy and Another v. Union of India and Others, Writ Petition (Civil) No. 494 of 2012 & Connected Matters*, 2018.
[62] AGID, *Regolamento eIDAS*, cit., art. 15.
[63] COM(2021) 281 final, cit., artt. 6-*bis*, 10, 15.
[64] European Commission, *The Digital Economy and Society Index*, 2022.
[65] Cfr. *Fatti e cifre sulla vita nell'Unione europea*.

* * *

Digital identity and protection of personal data: intersections and risks in the eIDAS and GDPR regulations

Abstract: The proposed amendment to the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) has reinvigorated the European debate on the issue of digital identity. The various problems that have emerged from this debate require better coordination of the proposal with pre-existing legislative instruments. This contribution aims to analyze the main points of friction between the regulatory framework related to electronic/digital identities and the European regulation concerning the protection of personal data.

Keywords: Electronic identity – Digital identity – eIDAS – GDPR