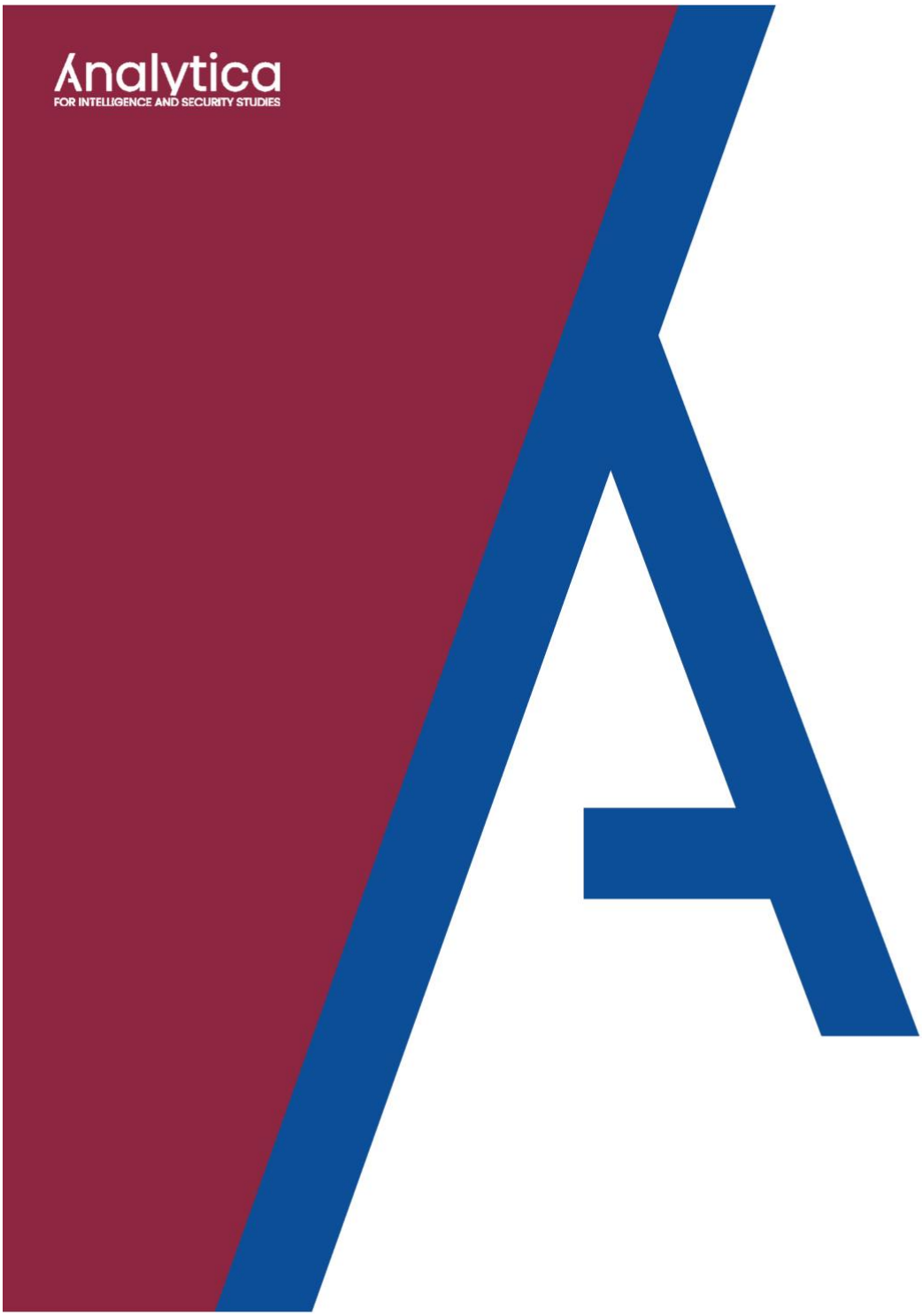

Identità digitale: opportunità e sfide per il conseguimento della trasformazione digitale.

Angela Lena

Analytica for intelligence and security studies

Paper Cyber-Security

ISSN: 2784-8779

Identità digitale: opportunità e sfide per il conseguimento della trasformazione digitale.

Angela Lena

Correzioni e revisioni a cura del Dottor SPELTA Maurizio

Direttore del Dipartimento Cyber – Security

Avv.to Maniscalco Davide.

Torino, luglio 2021

Stabilire la fiducia nell'utilizzo delle tecnologie digitali è un fattore determinante per una società che svolge gran parte delle interazioni e transazioni *online.* A tutti noi è capitato di dover fornire informazioni che ci riguardano per usufruire di un servizio o accedere ad un prodotto.
Che si tratti di aprire un conto in banca, acquistare prodotti soggetti a limiti di età o pagare le tasse, dimostrare la propria identità *online,* in maniera semplice e sicura, è la pietra angolare delle società digitali e delle economie future.

L'Europa ha una grande opportunità di diventare *leader* nella trasformazione digitale, ma ci sono esigenze concrete a cui deve rispondere. Tra queste, rientra l'identità digitale, una sfida che comprende non solo innovazione tecnologica, ma anche scelte politiche e considerazioni normative.
L'obiettivo da raggiungere è la creazione di un sistema di identificazione digitale fluido, efficiente e sicuro, che aumenti il livello di fiducia, oggi non più dipendente solo dagli investimenti in *advertising*, ma costruito sulla base dell'esperienza dell'utente e dal grado di sicurezza e affidabilità nella protezione delle informazioni personali.
Quando parliamo di *digital identity,* non c'è una sola ed unica via per creare fiducia, ma non si può prescindere da alcuni elementi chiave come, garantire la confidenzialità della comunicazione e far in modo che non sia alterata da soggetti non autorizzati; assicurarsi che le credenziali siano gestite da un ente affidabile e percepito come tale, e dalla garanzia che quando interagiamo con il sistema sia effettivamente quello legittimo. Il livello di fiducia è un elemento difficilmente quantificabile, ma è necessario lavorare su una politica di gestione delle identità digitali che sia riconosciuta come sicura e affidabile dagli utenti.
Se è vero, infatti, che oggi siamo in grado di compiere azioni che fino a qualche decennio fa erano solo nella mente di qualche visionario, la strada dell'innovazione è ancora lunga e non certo priva di rischi. In alcuni contesti, anche qualcosa di concettualmente semplice, come provare la propria identità, rimane un processo tutt'altro che snello e che spesso si configura come ripetitivo e dispendioso.

Per colmare queste lacune, una delle priorità strategiche in ambito europeo è quella di conseguire la **trasformazione digitale** e rendere il Digital Single Market (DSM) adatto all'era digitale. Tali obiettivi non potranno essere traguardati se lo sviluppo tecnologico a cui assistiamo non sarà accompagnato da solidi contrappesi in grado di salvaguardare i diritti degli utenti e i valori fondanti dell'Unione.

Lo scopo del presente lavoro è quello di mettere in luce alcune implicazioni di questa complessa sfida, per comprendere l'importanza dell'identità digitale e il suo significato per le moderne società. Cercheremo, dunque, di coglierne il potenziale senza però ignorare le sue criticità.

La pietra angolare per la competitività e il mercato unico dell'Europa

L'Unione europea ha un'ambizione ben precisa: conseguire la trasformazione digitale dell'Europa entro il 2030.
Non si tratta solo di una *vision* che punta a rafforzare la base economica, ma è qualcosa di più profondo, che riguarda la ridefinizione della sua identità nell'era digitale e la responsabilità di creare un **"futuro antropocentrico, sostenibile e prospero".**
Per tradurre questa ambizione in un programma concreto la Commissione, in risposta all'invito del Consiglio[1], ha presentato lo scorso 9 marzo una bussola digitale per indicare la rotta da seguire e realizzare la **leadership digitale europea.**
Il piano programmatica ruota intorno a quattro punti cardinali:

- cittadini dotati di competenze digitali e professionisti altamente qualificati nel settore digitale;
- infrastrutture digitali sostenibili, sicure e performanti;
- trasformazione digitale delle imprese;
- digitalizzazione dei servizi pubblici[2].

Se alcuni obiettivi non sembrano nuovi, c'è da dire che il *budget* per il bilancio europeo 2021-2027, è senza precedenti. Con un impegno da parte degli Stati membri a destinare almeno il 20% dei rispettivi piani di ripresa e resilienza, alla priorità digitale[3].

Il Digital Compass, dunque, individua uno degli strumenti per conseguire la transizione digitale nella *electronic identification* (eID), prevista per l'80% dei cittadini europei.

---

[1] Conclusioni del Consiglio europeo dell'1-2 ottobre 2020, EUCO 13/20.
[2] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni del 9 marzo 2021, 2030 DIgital Compass: the European way for the Digital Decade, COM (2021) 118 final.
[3] D. Maniscalco, *La Commissione Europea stabilisce la rotta per il decennio digitale. I 4 Punti.* in *Key4biz,* 15 marzo 2021, disponibile *online.*

La fruizione di **un'identità digitale verificata, unica, informata** (nel senso di un utilizzo consapevole) e soprattutto **sicura**, sarà **la pietra angolare delle economie future**, ed è su questo che si stanno concentrando gli sforzi dell'azione politica europea.

Non è la prima volta che l'Unione europea si trova ad affrontare il tema dell'eID e dei servizi fiduciari. Già nel 2014, con l'adozione del Regolamento eIDAS[4] (acronimo di *electronic IDentification, Authentication and trust Services*) entrato in vigore il 1° luglio 2016, ha mosso un importante passo verso l'interoperabilità tecnica e giuridica dei servizi fiduciari e dei mezzi di identificazione elettronica degli Stati membri. Con esso, si poneva l'obiettivo di instaurare la fiducia negli ambienti *online* e migliorare l'efficacia dei servizi elettronici sia pubblici che privati[5].

Il Regolamento eIDAS risponde a due esigenze importanti:

- garantire alle persone fisiche e giuridiche di poter utilizzare gli schemi nazionali di identificazione elettronica (eID), per accedere ai servizi pubblici *online* in altri paesi dell'UE. Il Regolamento, non richiede un unico Schema di identificazione europeo, ma il riconoscimento reciproco dei sistemi di identità nazionali, dando agli Stati membri la possibilità di notificare il proprio programma di identificazione elettronica alla Commissione[6]. La difficoltà in questo caso risiede nel fatto che non tutti i mezzi di identificazione hanno lo stesso livello di sicurezza e gli Stati che hanno previsto livelli di garanzia più elevati sono restii ad accettare Schemi considerati meno sicuri.
- creare un mercato interno europeo per i servizi fiduciari[7], ai quali è assicurato il funzionamento transfrontaliero e un'equiparazione ai modelli cartacei tradizionali.

---

[4] 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.

[5] Ivi, considerando 1 e 2.

[6] In Italia i due Schemi di identità nazionale notificati sono SPID (Sistema Pubblico di Identità Digitale) e CIE (Carta d'identità elettronica).

[7] Ai sensi dell'art. 3 del Regolamento (UE) n. 910/2014 per servizio fiduciario si intende: un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
b) creazione, verifica e convalida di certificati di autenticazione di siti web; o
c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Ad oggi, considerando il complesso degli Schemi di identificazione notificati, si può facilmente constatare come l'UE non sia ancora riuscita a cogliere tutto il potenziale dall'instaurazione di un'identificazione digitale efficiente e sicura. A titolo esemplificativo, notiamo come solo 15 Paesi su 27 abbiano garantito un'eID transfrontaliera ai propri cittadini, e come, nell'ambito dei singoli Stati, permangono significative disparità. Tra gli esempi virtuosi spicca l'Estonia, che ha implementato un sistema di identità digitale dal 2002, consentendo oggi al 99% della popolazione di avere una carta d'identità elettronica[8].

Le carenze strutturali dell'eIDAS sono oggetto di valutazione da parte della Commissione che, in virtù dell'articolo 49 del Regolamento, dopo quattro anni di vita, ha il compito di riesaminare la normativa alla luce degli sviluppi tecnologici e politici, per valutare l'impatto, la sua idoneità allo scopo ed apportare le conseguenti modifiche[9].
Nel documento *Proposal for a European Digital Identity (EUid) and Revision of the eIDAS Regulation*, vengono esposte tre opzioni per migliorare l'offerta e la domanda dei mezzi di identificazione digitale. Tutte e tre, in diversa misura, migliorerebbero lo stato attuale, ma l'impatto maggiore si avrebbe dalla combinazione della seconda e della terza opzione, vale a dire con l'estensione del Regolamento al settore privato (opzione 2) e con la creazione di un EUid universalmente accettato (opzione 3). A tal proposito, nelle già citate conclusioni dell'1 e 2 ottobre 2020, il Consiglio europeo ha chiesto alla Commissione di sviluppare un quadro a livello UE per l'identificazione elettronica pubblica e sicura, in modo da garantire alle persone **il controllo della loro identità e dei loro dati *online* e consentire l'accesso a servizi digitali pubblici, privati e transfrontalieri.** Pertanto, il 19 ottobre 2020, l'iniziativa EUid è stata inclusa nel programma di lavoro della Commissione 2021 ed è prevista per la prima metà di quest'anno.

SPID: stato dell'arte sull'utilizzo dell'identità digitale in Italia

L'Italia ha iniziato a muovere i primi passi verso la definizione di un sistema di identità digitali nel 2014, con un progetto ambizioso che ha visto la luce nel 2016 grazie al lavoro di AgID (Agenzia per l'Italia Digitale), e che conosciamo con il nome di Sistema Pubblico d'Identità Digitale - SPID, pensato per consentire l'accesso "*ai servizi online della pubblica amministrazione e dei privati*

[8] https://e-estonia.com/

[9] La Commissione ha avviato una consultazione pubblica, conclusa il 20 ottobre 2020, per raccogliere i pareri delle parti interessate sui fattori trainanti e sugli ostacoli allo sviluppo e alla diffusione dei servizi fiduciari e dell'eID in Europa e al momento della stesura del presente documento è in corso la revisione del Regolamento eIDAS.

*aderenti, con una coppia di credenziali (*username *e* password*) personali*"[10].
Al momento in cui si scrive, le identità SPID erogate in Italia sono 19.952.806[11]. Consultando i dati forniti da AgID, notiamo come esattamente un anno fa le identità erogate erano solo 6.581.535.

La tendenza positiva è da ricondurre principalmente a due fattori, il primo da ricercare nell'emergenza sanitaria dovuta al COVID-19, che ha contribuito ad accelerare il processo di digitalizzazione dei servizi pubblici, rendendo l'identità digitale uno strumento di distanziamento sociale e una misura per la tutela della salute pubblica. Il secondo è di natura legislativa, il c.d. Decreto Semplificazioni, convertito in legge con modificazioni dalla Legge 11 settembre 2020, n. 120, ha segnato una tabella di marcia per incrementare il livello di digitalizzazione nella pubblica amministrazione e "*favorire l'accesso ai servizi in rete da parte di cittadini e imprese e l'effettivo esercizio del diritto all'uso delle tecnologie digitali*"[12].

In particolare, l'art 24 del DL 76/2020 ha indicato il 28 febbraio 2021 come termine ultimo per lo *switch off* delle modalità diverse da SPID e CIE (Carta d'Identità Elettronica) per l'accesso ai servizi *online* delle pubbliche amministrazioni. Dalla stessa data è fatto divieto alle amministrazioni di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei cittadini ai propri servizi in rete, diverse da SPID, CIE o CNS (Carta Nazionale dei Servizi), fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il 30 settembre 2021[13].

Almeno nelle intenzioni, dunque, la previsione normativa ha l'obiettivo, da un lato di **semplificare la procedura per i cittadini,** non più legati alle innumerevoli e diverse credenziali necessarie per ogni servizio, dall'altro di **abbattere i costi** per gli enti pubblici e le amministrazioni che non devono più gestire i propri sistemi di rilascio delle identità.
Per far sì che tali obiettivi siano pienamente realizzati, all'aumento delle identità erogate deve far seguito anche un incremento dei servizi che consentano l'accesso tramite SPID, e che ad oggi secondo i dati ufficiali ammontano solo a 7.098[14].

---

[10] Definizione contenuta nel sito ufficiale.
[11] Il dato è relativo al 23 aprile 2021, secondo il monitoraggio dei progetti di trasformazione digitale effettuato dall'Agenzia per l'Italia Digitale e consultabile *online.* https://avanzamentodigitale.italia.it/it
[12] Decreto legge del 16 luglio 2020, n. 76 Misure urgenti per la semplificazione e l'innovazione digitale, art. 24, comma 1.
[13] Ivi, art. 24, comma 4.
[14] Il dato è aggiornato al 12/03/2021, consultabile *online.* https://avanzamentodigitale.italia.it/it#

Il quadro descritto non deve sorprendere, perché il processo di trasformazione digitale richiede risorse, economiche ed umane, oltre a competenze tecniche, che spesso mancano soprattutto nelle piccole realtà.

L'Italia è certamente sulla strada giusta e deve continuare a canalizzare gli sforzi in questa direzione, tuttavia, per sfruttare a pieno il potenziale del Sistema è necessario aumentare il livello di interazione *online* tra le autorità pubbliche e i cittadini, anche attraverso campagne volte non solo ad informarli sulle modalità per ottenere le credenziali, ma sulle potenzialità a cui esse sono preordinate, e definire delle strategie per potenziare la digitalizzazione dei servizi, non dimenticando le realtà più piccole[15].

Gap analysis dell'identificazione elettronica da remoto

Ai sensi del Cybersecurity Act, l'ENISA ha un ruolo importante nel supportare gli Stati membri e promuovere le migliori pratiche in tema di identificazione elettronica, e lo fa *"*[...] *fornendo consulenza e emanando orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti.*[16]" In virtù del suo ruolo, l'Agenzia europea ha pubblicato cinque reports al fine di rafforzare l'attuazione del regolamento eIDAS e promuovere l'adozione dell'identificazione elettronica e dei servizi fiduciari. Questi includono:

- frameworks di sicurezza per i fornitori di servizi fiduciari qualificati (QTSP) e fornitori di servizi fiduciari non qualificati (TSP);
- raccomandazioni sulla sicurezza per i fornitori di servizi fiduciari qualificati sulla base di standard;
- linee guida sulla valutazione della conformità dei fornitori di servizi fiduciari;
- un'analisi dei metodi utilizzati per eseguire il controllo dell'identità da remoto ed esplorare considerazioni sulla sicurezza.

[15] L'indice DESI 2020 colloca l'Italia al 19° nella dimensione Servizi Pubblici Digitali, dunque sotto la media europea, con solo il 32% degli utenti italiani che usufruisce attivamente dei servizi di e-government.

[16] Art. 5, par. 5 lett.a) del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

Nel documento Remote ID Proofing, l'Enisa ha sottolineato come l'impatto del COVID-19 abbia accelerato il processo di digitalizzazione in vista delle nuove esigenze, rendendo la possibilità di identificare una persona fisica a distanza, un fattore cruciale per lo sviluppo dei servizi transfrontalieri e la salvaguardia della salute pubblica.
L'Europa dovrà essere in grado di sfruttare tutto il potenziale che l'identificazione digitale ha da offrire, anche quando l'emergenza sanitaria sarà cessata, il che non potrà avvenire senza il coinvolgimento del settore privato e un'attenta mitigazione dei rischi da parte dei governi.

Come noto, l'identità di una persona è costituita da un insieme di attributi che permettono di identificarla in modo univoco in un determinato contesto. Quando questi attributi vengono acquisiti e archiviati elettronicamente parliamo di identità digitale, che dunque non è altro che la rappresentazione digitale di chi siamo, e il suo potenziale dipende dalle informazioni ad essa associate e dai servizi a cui permette di accedere[17]. Fermo restando che possono esserci diversi "set di attributi" che identificano in modo univoco detta persona"[18].
L'identificazione elettronica (eID) prevista dall'eIDAS, è una soluzione che fornisce la prova dell'identità per i cittadini e le organizzazioni, e che consente loro di accedere a servizi o effettuare transazioni *online.* Il livello di garanzia necessario dipende dalle attività per le quali l'identificazione è richiesta, non a caso l'art. 8 del Regolamento eIDAS prevede tre livelli di garanzia: basso, significativo ed elevato. Comprensibilmente, per le questioni sensibili, come il pagamento delle tasse o l'esercizio del voto, dove consentito, non saranno sufficienti *username* e *password* per provare la propria identità.
Tuttavia, è proprio in relazione al "remote ID proofing" che emergono diverse carenze, sia sul fronte normativo che su quello tecnico. Sotto il profilo giuridico, è innanzitutto la **mancanza di armonizzazione** tra i requisiti adottati dai singoli Stati membri che indebolisce l'ambizione europea. L'interoperabilità in questo campo è un obiettivo complesso da raggiungere, poiché deve far i conti con il diverso *background*, storico e culturale dei singoli Stati, che si sostanzia in una moltitudine di standard tecnici e quadri giuridici nazionali diversi.
Tra le cause della frammentazione degli approcci, si aggiunge anche un linguaggio a volte "aperto" del Regolamento stesso, basti pensare all'art. 24 "*Requisiti per i prestatori di servizi fiduciari qualificati*" e a come, ad esempio, è stato interpretato il requisito della presenza fisica di cui all'art.

[17] W. Echikson, *Europe's Digital Identification Opportunity*, in *Center for European Policy Studies,* 17 giugno 2020, reperibile *online.*
[18] Per esempio, si può far riferimento a dati biografici come, nome, età, sesso, indirizzo; oppure a dati biometrici, come impronte digitali e scansioni dell'iride, ma anche ad altri attributi che si riferiscono più in generale ad un aspetto della vita della persona.

24. 1, a), dai vari Stati membri[19].

Un margine di miglioramento è stato riscontrato anche sotto gli aspetti più tecnici, *in primis* riguardo la **mancanza di consapevolezza** da parte degli utenti circa la complessità del controllo d'identità da remoto e le sfide di sicurezza che esso pone. Una maggiore sensibilizzazione degli utenti aiuterebbe loro a comprendere meglio il flusso dei processi e a renderli più accorti alle minacce (ad es. ai tentativi di *phishing*).
Un altro ostacolo alla definizione di un processo uniforme, risiede nella **eterogeneità dei documenti fisici** su cui fanno affidamento i Paesi dell'Unione europea, e che spesso sono una parte essenziale dei metodi di verifica dell'identità a distanza. Ad esempio, secondo Eurosmart nel territorio dell'Unione esistono 86 carte d'identità diverse e 181 permessi di soggiorno[20]. Questa diversità si traduce in diversi livelli di affidabilità per i documenti rilasciati e che per questo motivo non consentono l'accesso a tutti i servizi in ogni Paese.

Quali sono i vantaggi della *digital ID*?

L'identità digitale è un prerequisito fondamentale per il *Digital Single Market* e in quanto tale dovrebbe essere tra le priorità di ogni agenda politica. L'Unione europea lo ha capito perfettamente, non a caso il suo obiettivo è quello di consentire a "*persone, imprese (in particolare PMI) e amministrazioni pubbliche di accedere in modo sicuro ai servizi e di effettuare transazioni online e transfrontaliere in un solo click.*[21]" La realizzazione di questo obiettivo avrebbe un impatto considerevole sulla vita di milioni di persone, garantendo loro comodità e sicurezza per molte operazioni *online* "*come la presentazione di dichiarazioni fiscali, l'iscrizione ad un'università straniera, l'apertura a distanza di un conto bancario, la creazione di un'impresa in un altro Stato membro, l'autenticazione per i pagamenti via Internet, la presentazione di offerte per un bando di gara online e altro ancora*"[22].

---

[19] Report dell'Agenzia dell'Unione europea per la sicurezza informatica (ENISA) dell'11 marzo 2021, Remote ID Proofing, p. 49, disponibile *online*.
[20] P. J. Verrando, *New EU eID cards regulation - a big move to keep a step ahead.* Presentation: The Identity Conference, Eurosmart, 2019, reperibile *online*.
[21] European Commission, *Trust services and electronic identification*, 4 Marzo 2021, reperibile *online*.
[22] *Ibidem*.

Oltre a questi vantaggi, un sistema di identità digitale porta con sé dei benefici anche in termini di crescita economica. Da un'analisi di Mckinsey emerge che l'implementazione di un *digital ID* nel 2030, avrebbe il potenziale per sbloccare un valore economico pari al 6% del PIL nelle economie emergenti e al 3% nelle economie più mature[23].

Ad ogni modo, sbloccare il valore potenziale di un sistema di identificazione digitale non è affatto certo o automatico, piuttosto si configura come l'esito di un processo complesso che deve affrontare molteplici aspetti, tra cui quello della fiducia. Infatti, se nei metodi tradizionali, come le identità cartacee, la fiducia era garantita dai governi, nelle identità digitali dovrà essere costruita sul rispetto di una *governance* costantemente aggiornata, sulla definizione di regole per la protezione della privacy e meccanismi che rendano l'utente informato su come i suoi dati vengono protetti. Il processo di costruzione della fiducia non richiede soltanto di compiere decisioni in materia di sicurezza, ma anche di adottare la giusta strategia per comunicare tali decisioni al pubblico e creare un rapporto sinallagmatico in cui "il corrispettivo" che si ottiene è la fiducia nelle tecnologie digitali.
La creazione di *ID system* è anche ampiamente riconosciuta come strumentale per l'accesso a diritti fondamentali e la realizzazione di una crescita sostenibile, soprattutto nei Paesi in via di sviluppo. La Banca Mondiale ha presentato delle linee guida su come un "*good ID*", cioè un sistema di identificazione inclusivo e affidabile, possa essere un fattore abilitante per la realizzazione di uno dei traguardi degli Obiettivi per lo Sviluppo Sostenibile (*Sustainable Development Goals*, SDGs) di "non lasciare indietro nessuno"[24].

Quali i problemi?

Ogni tecnologia porta con sé dei rischi che devono essere identificati, valutati, analizzati e gestiti. Tra questi rientra innanzitutto **un uso improprio dei sistemi di identificazione digitale,** che potrebbero essere sfruttati per il perseguimento di fini illeciti. Per far fronte a ciò è necessario incorporare disposizioni sulla privacy sin dalla progettazione delle infrastrutture di identificazione elettronica (ad es. integrando il principio di minimizzazione) e prevedendo dei meccanismi per la creazione del consenso dell'utente e il controllo dei suoi dati.

---

[23] O. White, A. Madgavkar, J. Manyika, D. Mahajan, J. Bughin, M. McCarthy, e O. Sperling, *Digital identification: A key to inclusive growth*, in *McKinsey Global Institute*, 17 aprile 2019, reperibile *online*.
[24] The World Bank Group, *Good ID supports multiple development goals*, ID4D publications, reperibile *online*.

Le conseguenze che possono derivare da una violazione della privacy di tali sistemi sono molteplici, dal furto e uso improprio dei dati, al furto d'identità o al compimento di atti discriminatori. Per questo motivo, la previsione di un *risk assessment* della privacy appare fondamentale. Ad esempio, conducendo una valutazione di impatto sulla protezione dei dati personali (DPIA), si possono individuare e mitigare i rischi associati al trattamento dei dati personali.

Un altro fattore che deve essere preso in considerazione è il rischio che la creazione di un nuovo sistema di identificazione possa generare fenomeni di **esclusione sociale**, per esempio subordinando l'accesso al voto al possesso di una specifica credenziale digitale, a tal proposito si devono valutare attentamente i rischi di emarginazione delle categorie più vulnerabili e implementare strategie per garantire l'accesso all'identificazione a tutti[25].

Di fondamentale importanza è anche la **scelta tecnologica** compiuta. Durante il processo di progettazione del sistema, è necessario valutare anche i rischi legati alla tecnologia che si sceglie di utilizzare e la sua sostenibilità nel tempo.

Conclusioni

Per costruire un sistema di identificazione digitale che promuova un mercato competitivo e rispetti i diritti fondamentali, si devono compiere scelte politiche, considerazioni normative e valutazioni tecniche sfidanti.

La prova dell'identità di una persona *online* deve essere il risultato di un **processo snello** ma anche **inclusivo**, **affidabile** e **sicuro**, solo così si potrà stabilire la fiducia nei servizi digitali e realizzare pienamente il *Digital Single Market.*

Questi obiettivi non sono stati ancora traguardati e, all'interno dell'Unione si registra una sostanziale disparità nell'utilizzo dell'eID, con quasi il 98% dei servizi pubblici disponibili in Paesi nordici come Finlandia ed Estonia, e meno del 40% in Romania, Bulgaria e Grecia.

Per "plasmare il suo futuro digitale", l'Europa deve agire senza ulteriori indugi e rispondere ad esigenze concrete. È necessario andare oltre il disegno iniziale[26] e **coinvolgere il settore privato** per migliorare l'efficienza e la scalabilità dei sistemi di identificazione, assicurando al contempo un'attenta gestione dei rischi derivanti da siffatta collaborazione[27].

---

[25] The World Bank Group, *Creating a good ID system presents risks and challenges, but there are common success factors*, ID4D publications, reperibile *online.*

[26] Oggi solo i governi possono notificare gli schemi di eID.

[27] J. Clark, M. Dahan, V. Desai, M. Ienco, S. de Labriolle, J-P. Pellestor, Y. Varuhaki, K. Reid, "*Digital Identity : Towards Shared Principles for Public and Private Sector Cooperation*", World Bank Group-GSMA, luglio 2016, reperibile *online.*

Un esempio virtuoso di *public-private partnership* è il caso eHerkenning dei Paesi Bassi[28], che ha sostituito i molteplici set di chiavi digitali utilizzati dal governo olandese, e che avevano di fatto frenato la crescita dell'e-Business e dell'e-Government, con un'unica "*master key*" che permette alle organizzazioni di rendere accessibili, in tutta sicurezza, i propri servizi *online*[29].

Oltre al coinvolgimento delle diverse parti interessate, i sistemi di identificazione elettronica sono progetti ambiziosi che richiedono una solida base per la loro riuscita. Innanzitutto, **la protezione dei dati** deve seguire un approccio *by-default*, e quindi deve essere considerata sin dalle fasi di progettazione dei sistemi. È, inoltre, necessario incoraggiare un'innovazione tecnologica che metta al centro l'utente, la semplicità e la protezione dei dati[30].

In un mondo interconnesso la capacità per gli individui e le organizzazioni di comunicare in modo sicuro assume un ruolo fondamentale, per questo motivo la nuova strategia dell'UE per il decennio digitale ha l'obiettivo di far sì che tutti siano in grado di vivere in sicurezza la propria vita *online*. In quest'ottica va menzionato un obiettivo importante nella *roadmap* per la trasformazione digitale, vale a dire la volontà dell'Europa di dotarsi del primo computer con accelerazione quantistica entro il 2025 e di essere all'avanguardia nelle capacità quantistiche entro il 2030[31]. Il 20 aprile 2021 a Maribor, in Slovenia, è stato inaugurato Vega, il primo degli otto super-computer che l'UE ha pianificato di acquisire e distribuire sul suo territorio nell'ambito del proficuo partenariato pubblico-privato EuroHPC.

Nel Digital Compass, la rivoluzione quantistica è presentata come un punto di svolta per lo sviluppo e l'utilizzo delle tecnologie digitali così come le conosciamo oggi. L'impiego dei sistemi di comunicazione quantistica, infatti, potrebbe aumentare la sicurezza delle comunicazioni e dei trasferimenti di dati, e avere un impatto sui sistemi di voto online, sulle transazioni finanziarie e molto altro ancora. Verosimilmente, dunque, il loro avvento inciderà anche sugli algoritmi di crittografia in uso e il loro attuale impiego. Se infatti un computer classico incontra difficoltà nel "rompere" un sistema crittografico a chiave pubblica, oggi largamente utilizzati nei protocolli di sicurezza, un computer quantistico, teoricamente, riuscirebbe nella stessa operazione in pochi secondi.

---

[28] https://www.eherkenning.nl/english/public-prive-cooperation

[29] https://www.eherkenning.nl/english

[30] Molto interessante a questo proposito è il report della dott.ssa Michèle Finck per il Parlamento europeo sul rapporto tra Blockchain e il Regolamento Ue 2016/679. M. Finck, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*, in *EPRS | European Parliamentary Research Service*, luglio 2019, reperibile *online*.

[31] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, del 9 marzo 2021, 2030 Digital Compass: the European way for the Digital Decade COM(2021) 118 final, p. 8.

Si pone dunque la necessità di sviluppare una post-quantum cryptography, vale a dire algoritmi resistenti all'avvento dei computer quantistici[32].

L'identità digitale si basa su molte tecnologie, tra cui la stessa crittografia, per questo motivo è importante analizzare il suo utilizzo nella gestione delle infrastrutture e cercare di comprendere i possibili sviluppi futuri.

Ad ogni modo, quando parliamo di identità digitali, il *leitmotiv* dovrebbe essere l'aumento del livello di fiducia, tra coloro che devono dimostrare chi dicono di essere e la parte che fa affidamento sull'identificazione elettronica (*relying party*)[33]. Questa fiducia si nutre della garanzia di un sistema inclusivo e che abbia a cuore la sicurezza degli utenti e il rispetto dei loro diritti, senza privarli dell'efficienza e dell'innovazione che le tecnologie digitali possono offrire.

Come ricorda sapientemente Phillip Windley, è difficile provare la fiducia tramite un algoritmo, ma è l'elemento chiave per il successo di qualsiasi sistema di identità digitale[34].

[32] L'agenzia statunitense NIST (National Institute of Standards and Technology) sta lavorando ad uno standard di post-quantum cryptography che dovrebbe vedere la luce nel 2024.

[33] Art. 3, n. 6), Regolamento Regolamento (UE) n. 910/2014.

[34] Phillip J. Windley, *Identità digitali*, maggio 2006, pp. 15 ss.