Università
Ca'Foscari
Venezia

Corso di Laurea magistrale

in Governance delle Organizzazioni Pubbliche

Tesi di Laurea

Verso una cittadinanza digitale

Innovazione e digitalizzazione nella Pubblica Amministrazione

Relatore

Ch. Prof. Agostino Cortesi

Laureanda

Giulia Schiff

Matricola 859569

Anno Accademico

2019/2020

Ipsa scientia potestas est.

- Sir Francis Bacon

Indice dei contenuti

Introduzione……..7

CAPITOLO I: Non solo identità digitali: il quadro……9

1.1 L'identità digitale…….10

1.2 Le firme…….12

1.3 La posta elettronica certificata (PEC)……14

1.4 La marca temporale……..…15

CAPITOLO II: La normativa europea e internazionale…….…….17

2.1 Il regolamento eIDAS (2014/910/EU)…….…….17

2.2 Regolamento di esecuzione 2015/1501/EU, regolamento 2016/679/EU e regolamento 2018/1724/EU……..……..21

2.3 L'Agenzia dell'Unione europea per la cybersicurezza e il regolamento 2019/881/UE…….…….24

2.4 L'Istituto Europeo per gli Standard nelle Telecomunicazioni (ETSI) …….…….25

2.5 L'Organizzazione Internazionale per la Standardizzazione (ISO)…..……..27

CAPITOLO III: La normativa nazionale……..……29

3.1 Il Codice dell'amministrazione digitale (CAD)…….…….29

3.2 L'Agenzia per l'Italia Digitale (AgID)…….……31

3.3 I piani per l'innovazione e l'informatica nella Pubblica Amministrazione……32

3.4 Il documento informatico: nuove linee guida…….35

CAPITOLO IV: Strumenti per l'innovazione e la digitalizzazione in Italia…….39

4.1 Sistema Pubblico di Identità Digitale (SPID)……..40

4.2 Carta d'Identità Elettronica (CIE)…….…42

4.3 Carta Nazionale dei Servizi (CNS)……..…….44

4.4 Anagrafe Nazionale Popolazione Residente (ANPR)……45

4.5 PagoPA……..46

4.6 Fatturazione elettronica……..……48
4.7 "IO" app……49
4.8 Sanità digitale……..51
4.9 Cloud della PA……52
4.10 Public e-Procurement……53
4.11 Avanzamento della trasformazione digitale in numeri (ottobre 2020)……..54
CAPITOLO V: I progetti europei……57
5.1 I progetti STORK e STORK 2.0……..57
5.2 Due progetti sul principio once-only: TOOP e SCOOP4C……61
5.3 Sfide sulla protezione dei dati personali: PoSeID-on……66
CAPITOLO VI: L'uso delle eID e degli eServices nelle Pubbliche Amministrazioni….71
6.1 Il caso dell'Estonia: uno Stato all'avanguardia……..73
6.2 Il modello della Spagna e di Barcellona……..80
6.3 Milano: un esempio virtuoso nel contesto italiano……86
CAPITOLO VII: Elementi di criticità, barriere e considerazioni…….…..91
7.1 Molteplicità identità digitali e correlazione servizi digitali - eID……91
7.2 Servizi transfrontalieri e lingue di comunicazione……92
7.3 Ulteriori fattori di esclusione: età e difficile comprensione……..93
7.4 Percezione, fattori socio-culturali e coinvolgimento del settore privato…….94
7.5 eGovernment e blockchain……95
7.6 Dubbi sui metodi di riconoscimento……96
7.7 Complicazioni nell'autenticazione e sicurezza……..97
7.8 Incidenti di sicurezza 2019 (report ENISA 2020)……98
Conclusioni……..101
Fonti……..105

Introduzione

Negli ultimi vent'anni c'è stata una profonda evoluzione sul fronte della digitalizzazione del settore pubblico tanto che in alcuni casi si potrebbe parlare anche di cittadinanza digitale. È aumentato notevolmente il numero di servizi pubblici on-line, e quindi sono stati perfezionati se già presenti, o adottati in molti altri casi, sistemi di autenticazione sicura in rete: le cosiddette identità digitali (eID). Queste costituiscono un sistema identificativo univoco sul web, al pari della carta d'identità o del passaporto nel mondo fisico, e per questo si stanno rivelando fondamentali data la sempre maggiore diffusione di beni tecnologici e del contesto di semplificazione che richiedono i cittadini europei nel momento in cui si rivolgono alle Pubbliche Amministrazioni. L'Unione europea infatti ha predisposto un piano per l'eGovernment 2016-2020 a favore della digitalizzazione della Pubblica Amministrazione, da conseguire semplificando e rimodernando i processi interni, rendendo possibile usufruire dei servizi in modalità transfrontaliera, e favorendo dinamiche di co-creazione.

Le eID, essendo nate nei singoli contesti nazionali, hanno standard e metodi di funzionamento diversi. Per questo, nel corso dell'ultimo decennio è nata la necessità di creare una base comune di interoperabilità per raggiungere l'obiettivo europeo del mercato unico anche verso i servizi pubblici di ciascuno Stato membro. A questo proposito allora si collocano due tra i principali regolamenti a livello europeo che hanno dato inizio alla strada verso il riconoscimento reciproco delle identità digitali tra Stati e a principi comuni sulla protezione dei dati personali: parliamo del regolamento eIDAS del 2014 e del General Data Protection Regulation del 2016. Sempre nel contesto europeo va ricordata la Dichiarazione Ministeriale sull'eGovernment di Tallinn per i principi, tra gli altri, di inclusività, sicurezza, protezione dei dati personali e principio once-only.

L'obiettivo di questo elaborato è quindi quello di ricostruire il contesto intorno all'evoluzione della digitalizzazione degli ultimi anni, individuare lo stato dell'arte odierno in Italia e in Europa e presentare alcune buone pratiche da cui potenzialmente poter prendere spunto. Il focus globale che guiderà il lettore sarà principalmente quello delle identità digitali e dei servizi pubblici on-line. Inoltre, l'auspicio è che il risultato possa essere utile ai dipendenti pubblici che si approcciano per la prima volta al tema e che sono curiosi di approfondire il contesto di riferimento.

La stesura dell'elaborato è improntata su una metodologia di tipo compilativo. La ricerca del materiale è stata rivolta principalmente verso canali istituzionali e articoli accademici. I risultati ottenuti hanno evidenziato da una parte la sempre maggiore necessità di usufruire di servizi pubblici digitali senza confini e di incrementare la semplificazione nel rapporto con le Pubbliche Amministrazioni; dall'altra, oltre ai casi in cui è chiaro il ritardo nei processi di digitalizzazione e che quindi presentano mancanze importanti, emergono pur sempre delle riserve in merito alla sicurezza e alla protezione dei dati e infine la presenza di ostacoli a cui inevitabilmente portano le soluzioni digitali.

La struttura del testo è composta essenzialmente da due parti. Nei primi tre capitoli si andrà a circoscrivere il tema, trattando in primis le identità digitali e altri strumenti utili allo sviluppo dell'uso delle soluzioni digitali. Poi verrà analizzata la struttura normativa europea e italiana. Nella seconda parte, dal capitolo quattro al sette, si descriveranno gli strumenti utilizzati in Italia, alcuni progetti europei di particolare interesse e tre esempi di amministrazioni dove l'elemento digitale e le eID sono ormai una parte integrante del sistema. Infine si vedranno i principali elementi di criticità e le barriere a uno sviluppo diffuso delle identità digitali.

CAPITOLO I

Non solo identità digitali: il quadro

"La rivoluzione industriale del nostro tempo è digitale", così afferma Andrus Ansip, ex vicepresidente della Commissione europea e responsabile per il mercato unico digitale. Come le aziende in passato, anche i servizi pubblici sono chiamati ad entrare nel mercato unico che è pensato per essere caratterizzato come digitale, aperto e transfrontaliero. Sono ormai più di dieci anni che si parla assiduamente di digitalizzazione e di eGovernment: vogliamo ricordare in particolare la Dichiarazione di Malmö (2009), l'eGovernment Action Plan 2016-2020 e la Dichiarazione Ministeriale sull'eGovernment di Tallinn (2017) come i manifesti europei trainanti di questa "rivoluzione". In particolare da Tallinn emergono principi come il digital by default, l'inclusività, l'accessibilità, il principio once-only, la sicurezza, la trasparenza e l'interoperabilità. L'idea di eGovernment (o amministrazione digitale) si basa su un netto incremento dell'efficienza, da cui consegue necessariamente un risparmio per imprese e Pubbliche Amministrazioni, maggiore trasparenza, e per ultimo, ma non meno importante, maggiore partecipazione del cittadino alla vita politica. Se volessimo descrivere l'eGovernment usando una sola parola, allora sarebbe appropriato scegliere "semplificazione": in fin dei conti se le Pubbliche Amministrazioni devono essere al servizio dei cittadini, facilitare la vita pubblica risulta necessario e irrimandabile alla luce delle complessità della nostra epoca. Ma all'interno delle eterogenee dinamiche pubbliche, innovare costa fatica, e quindi richiede tempo. Tuttavia, la tecnologia, secondo la strategia europea, non può più essere una barriera, ma deve farsi strada come uno strumento e un valore aggiunto a favore dei cittadini. Ecco allora che si avvicina il tempo della "cittadinanza digitale", dove elementi innovativi vengono posti al servizio di cittadini, imprese e Pubblica Amministrazione per agevolare i rapporti che intercorrono tra loro. A questo proposito, esistono diverse tipologie di strumenti che

permettono di operare o accedere al mondo digitale. Di seguito ne vengono proposti i principali.

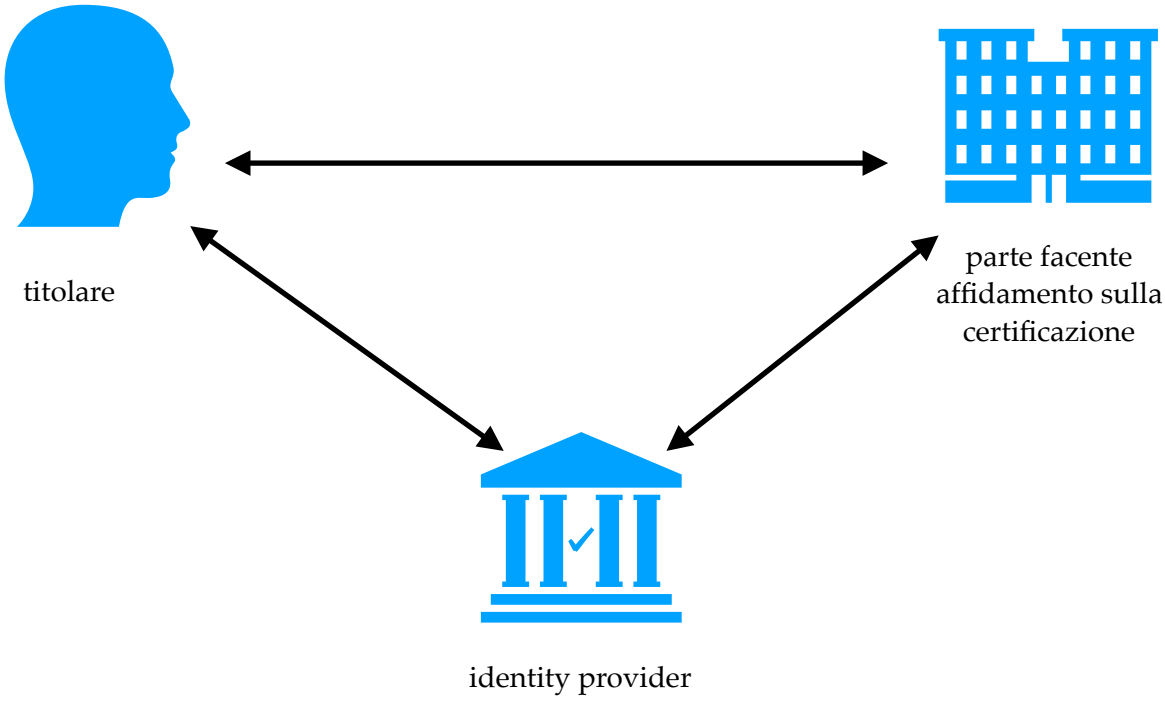
1.1 L'identità digitale

Se un documento identificativo cartaceo serve a provare l'identità di una persona nel mondo fisico, lo stesso deve essere possibile anche in un contesto elettronico, dove a fronte dell'incremento nell'uso di Internet, risulta necessario avere ben chiaro chi siano le parti coinvolte. A questo proposito si prestano i mezzi d'identificazione elettronica (eID). Secondo il Codice dell'amministrazione digitale (CAD), un'identità digitale è "la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale" [1, articolo 1]. Ciò vale a dire che a una persona viene associata in modo univoco una corrispondente identità digitale, previa autenticazione da parte di un ente abilitato, l'identity provider. L'identity provider si occupa di verificare i dati forniti e si accerta che l'utente che richiede l'identità digitale sia davvero chi afferma di essere, e una volta appuratolo può rilasciare l'identità digitale. L'utente poi potrà far uso dell'identità digitale per accedere ai servizi on-line, siano essi pubblici o privati, che richiedono un'identificazione elettronica. Inoltre, l'utente risponde in prima persona nel caso in cui si verifichi un uso non previsto dell'eID, e non può cedere a terzi l'uso dell'identità. Dall'altra parte, al titolare del servizio (o parte facente affidamento sulla certificazione) vengono comunicati dall'identity provider i dati dell'utente idonei ad assolvere alla richiesta, quali ad esempio nome, cognome, data e luogo di nascita, codice fiscale, e contatto e-mail.

Sul fronte della sicurezza, una eID presenta tre diversi livelli di garanzia, che possono essere attivati o meno dall'utente in base ai servizi di cui fa uso. Infatti, non è sempre richiesto il livello massimo di garanzia, dato che spesso questo è associato a una minore facilità d'uso e a costi maggiori. Per acquisire il secondo livello ad

esempio, l'utente richiedente è sottoposto a un vero e proprio riconoscimento che può essere effettuato con un colloquio di persona oppure mediante video identificazione con un operatore, ma sempre basandosi su un documento identificativo cartaceo. In generale, ogni livello di sicurezza richiede un ulteriore fattore di autenticazione.

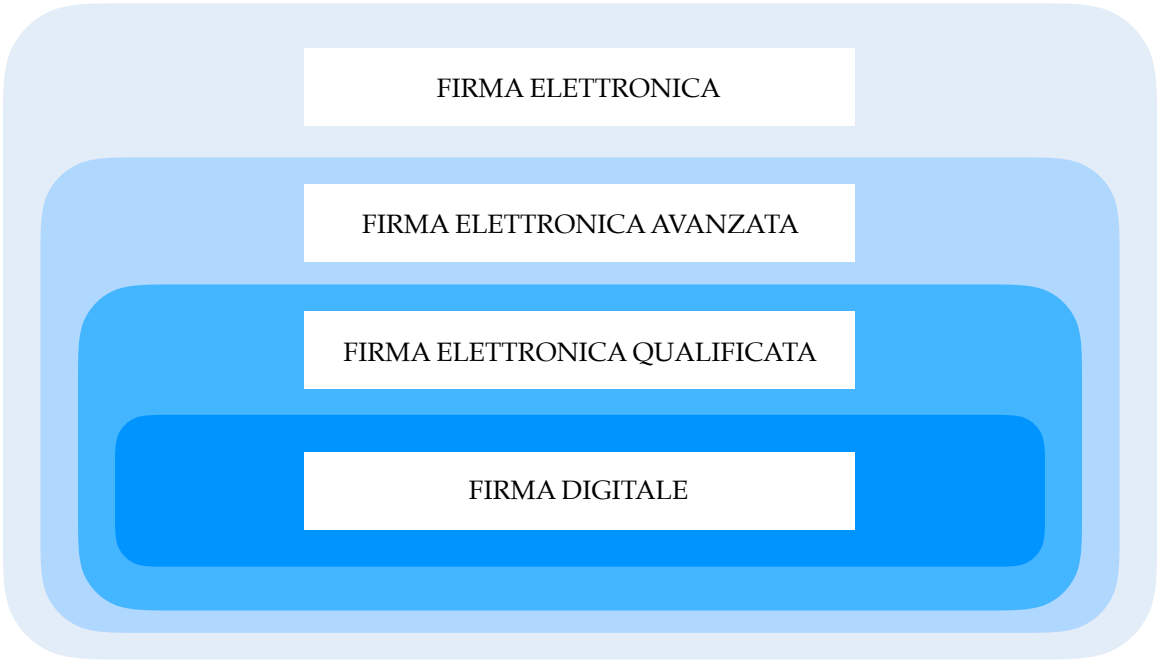
Per concludere, la peculiarità dell'uso di un'identità elettronica sta nel fatto che è possibile accedere ai servizi disponibili mediante le stesse credenziali, quindi non è più necessario ad esempio ricorrere alla registrazione a ciascun singolo sito internet, ma verranno sfruttati i benefici di un'unica identità digitale. Per il futuro sono previste ulteriori applicazioni da sfruttare in ambito di eGovernment.



Rapporti a tre che si producono nel contesto delle eID [29]

1.2 Le firme

Vi sono differenti categorie di firme valide nel contesto italiano utili ad autenticare un documento elettronico: la firma elettronica semplice, la firma elettronica avanzata, la firma elettronica qualificata e la firma digitale.



Le tipologie di firme [4]

La firma elettronica semplice viene rappresentata come un insieme di dati in forma elettronica "acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare" [2, articolo 3]. Più semplicemente, si tratta di una correlazione tra dati e documento elettronico per l'autenticazione informatica di quest'ultimo. Un esempio può essere il codice PIN, oppure la combinazione di nome utente e password usate per avere accesso a un sito internet. Tuttavia questo non risulta sufficiente per garantire la sicurezza in quanto non vengono assicurati autenticità, non ripudio e integrità del documento [3].

La firma elettronica avanzata (FEA) fa un passo ulteriore verso il miglioramento delle caratteristiche di sicurezza. Deve essere connessa unicamente al firmatario e quindi essere idonea ad identificarlo; inoltre, i dati usati per la sua

creazione devono essere detenuti unicamente dal firmatario e devono essere collegati alla firma per permettere di individuare eventuali variazioni dei dati stessi [2, articolo 3 e 26]. Un esempio calzante è la firma grafometrica su tablet. In questo caso, all'atto della firma vengono acquisiti tutta una serie di dati biometrici del firmatario, come la posizione con cui viene tenuto il pennino, la velocità, il ritmo e la pressione di firma. I dati biometrici vengono allora uniti e vincolati alla firma apposta al documento [3]. Questa tipologia di firma presenta una vasta gamma di dati al suo interno ed è quindi più sicura di una firma autografa classica che al contrario può essere soggetta a distorsioni e contraffazioni.

La firma elettronica qualificata (FEQ) è un caso particolare di firma elettronica avanzata, "creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche" [2, articolo 3]. Giuridicamente parlando, la firma elettronica qualificata è equiparata a tutti gli effetti a una firma autografa [2, articolo 25]. Gli elementi essenziali che quindi costituiscono questo tipo di firma sono il certificato e il dispositivo di firma qualificato. Il certificato serve a tracciare una linea univoca tra il nome o lo pseudonimo del firmatario fisico e i dati di convalida, mentre il dispositivo è l'elemento che permette a tutti gli effetti la sottoscrizione di un documento informatico. Il compito del dispositivo di firma qualificato può essere soddisfatto da una smart card, una chiavetta USB o un token. Tutto questo permette di ottenere una garanzia univoca sull'identità del firmatario [3]. Uno strumento simile alla firma elettronica qualificata è il sigillo elettronico qualificato che si distingue per il fatto che si riferisce a una persona giuridica, quindi risulta più adatto all'uso di enti o aziende [4].

Infine vi è un ultimo caso particolare, la firma digitale, tipologia che deriva dalla firma elettronica qualificata. La firma digitale è presente solo in Italia ed è basata su un sistema di chiavi crittografiche collegate tra loro, una pubblica e una privata. Sostanzialmente, il firmatario firma con la chiave privata il documento, e un soggetto terzo sarà in grado di verificare la provenienza del documento utilizzando la chiave pubblica associata in maniera univoca al firmatario [1, articolo 1 e 24].

Questo processo è conosciuto come crittografia asimmetrica e consente un elevato livello di sicurezza, per questo è sempre stata privilegiata dal legislatore italiano [3].

1.3 La posta elettronica certificata (PEC)

La posta elettronica certificata (PEC) è un sistema che permette la trasmissione telematica di messaggi aventi lo stesso valore legale di una raccomandata con ricevuta di ritorno. L'invio di un messaggio si reputa posta certificata solo se entrambi mittente e destinatario utilizzano caselle di posta certificata. Il meccanismo di scambio dei messaggi funziona mediante la creazione di ricevute e buste di trasporto. Quando viene inviato un messaggio, il gestore del mittente gli invia una ricevuta di accettazione firmata comprendente l'orario di spedizione e i destinatari, e poi procede a creare una busta di trasporto, contenente il messaggio originale, i dati di spedizione e la firma del gestore. Questo processo permette poi al gestore del destinatario di accertare l'effettiva integrità del messaggio. Quando il destinatario riceve il messaggio, il gestore del destinatario provvede a inoltrare al mittente una ricevuta di consegna firmata che assicura se la consegna sia avvenuta o meno, l'ora e la data di consegna e infine il contenuto del messaggio, completo di eventuali allegati. La ricevuta di consegna consente al mittente di avere prova che il messaggio invitato è stato ricevuto nella sua totalità [5]. In Italia è obbligatorio dotarsi di PEC per imprese, liberi professionisti iscritti agli albi e Pubbliche Amministrazioni. I relativi indirizzi di posta sono reperibili presso i portali INI-PEC per imprese e liberi professionisti e presso iPA per le Pubbliche Amministrazioni.

Un'evoluzione della PEC sono i servizi elettronici di recapito certificato qualificati (SERCQ), e pur essendo previsti dal legislatore europeo non sono ancora utilizzati in Italia. Le peculiarità stanno nell'identificazione del destinatario prima del recapito dei dati per mezzo di identità digitali, un elevato livello di sicurezza per

l'identificazione del mittente e la possibilità di trasferire allegati di dimensione più elevata [6 e 7].

1.4 La marca temporale

La marca temporale è uno strumento che apposto a un documento informatico, digitale o elettronico ne certifica la data e l'ora di emissione rifacendosi al tempo universale coordinato mediante una sequenza di caratteri creati da un ente accreditato chiamato Time Stamping Authority (TSA). Può essere apposta anche a file non firmati digitalmente permettendo così di validarli legalmente. Il processo di marcatura temporale è utile nel momento in cui si vuole definire con sicurezza un momento preciso e certo a partire da cui un documento informatico ha valore legale, consentendo di estenderne la validità nel tempo per un periodo non inferiore a vent'anni [8].

CAPITOLO II

La normativa europea e internazionale

Per circoscrivere in maniera efficace tutto ciò che si raggruppa negli strumenti e nelle identità digitali, è necessario e doveroso andare ad esplorare l'ambito normativo. Il contesto europeo, come abbiamo visto, è ricco di materiale e spunti per incrementare la crescita del mondo digitale, e si pone costantemente obiettivi da raggiungere, perché è cosciente che il cambiamento non accade in pochi giorni, ma è dato da un lungo processo da percorrere a piccoli passi.

In questo capitolo allora ci interesseremo di ciò che emerge a livello internazionale: esamineremo innanzitutto i regolamenti europei più essenziali, e poi daremo uno sguardo all'importanza degli standard internazionali. Le parole chiave attorno a cui si focalizzano le normative esposte sono interoperabilità e sicurezza informatica, senza dubbio tra le priorità per il buon funzionamento di un mercato unico digitale. Tuttavia, pur essendoci molto materiale a disposizione, questo spesso appare generale e sotto alcuni aspetti ridondante, e pertanto vi è grande margine di manovra lasciato ai singoli Stati, aspetto che a tratti potrebbe minare l'intenzione di raggruppamento e coesione dei sistemi digitali europei.

2.1 Il regolamento eIDAS (2014/910/EU)

Il regolamento europeo 2014/910/EU, meglio conosciuto come eIDAS, e che entra in vigore a partire dal 1° luglio 2016, è forse il più importante regolamento sull'argomento e si pone come pietra miliare da cui partire per tutto quello che viene dopo. Ha il compito di iniziare a ordinare un quadro abbastanza eterogeneo e confuso riguardo l'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno, e quindi di andare ad aggiornare la normativa

relativa alle firme elettroniche abrogando la direttiva 1993/93/CE, ormai superata per la mancanza di un quadro transfrontaliero e completo.

Se facciamo un passo indietro, le premesse che portano alla necessità di regolamentazione si rivolgono per lo più alla crescente necessità di instaurazione di fiducia negli ambienti online, per facilitare una base condivisa atta a favorire interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche. Questa base comune è fortemente voluta, in quanto mira a indirizzarsi verso uno sviluppo economico e sociale di un mercato unico digitale che ancora mancava all'interno dell'Unione. Già nel 2010, con l' "Agenda digitale europea", la Commissione europea aveva discusso di problematiche come la frammentazione del mercato digitale, la mancanza di interoperabilità e un crescente aumento della criminalità cibernetica, tutti elementi che rischiavano di minare la fiducia nel mercato digitale in espansione. Tempo addietro invece, con la direttiva 2006/123/CE, era stato chiesto agli Stati di sviluppare degli "sportelli unici" utili allo svolgimento a distanza e in formato elettronico di attività e servizi, mentre con la direttiva 2011/24/UE si chiedeva di creare una rete di autorità nazionali con il compito di guidare l'assistenza sanitaria online verso un'agevolazione della trasferibilità dei dati a favore dell'assistenza sanitaria transfrontaliera, cosa che poi ha portato in un contesto più ampio alla creazione del fascicolo sanitario elettronico.

A dispetto di questa forte volontà di coordinamento e innovazione, mancava però ancora un riconoscimento reciproco dell'identità elettronica di un cittadino in un Paese che non fosse il suo, cosa che si presentava come limite al godimento dei vantaggi del mercato interno e che impediva un regime di riconoscimento reciproco. Vi era anche la necessità di coinvolgere il settore privato nell'impiego volontario dei mezzi di identificazione elettronica.

Quello che emerge come obiettivo focale non si propone però di intromettersi nei sistemi che gestiscono le identità elettroniche e tantomeno nelle infrastrutture presenti negli Stati membri, ma si vuole arrivare ad assicurare metodi di

identificazione e autenticazione elettronica sicura nel momento in cui si fa uso di servizi online transfrontalieri.

Il regolamento nel suo insieme risulta diviso in sei capi. Si inizia volendo delineare mediante definizioni i concetti principali legati alla trattazione dell'identificazione elettronica e dei servizi fiduciari (Trust Services — TS). Tra le definizioni presenti nel capo I viene subito precisato, tra le altre, la nozione di "identificazione elettronica" come "il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica" [2, articolo 3]. Un'altra importante definizione che viene riportata è quella di "servizio fiduciario", "un servizio elettronico fornito normalmente dietro remunerazione e consistente…[nella] 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 [nella] creazione, verifica e convalida di certificati di autenticazione di siti web, o [nella] conservazione di firme, sigilli o certificati elettronici relativi a tali servizi" [2, articolo 3].

Al capo II troviamo la parte sull'identificazione elettronica che comprende una grande novità: il riconoscimento reciproco. Infatti, qualora vi sia un'autenticazione elettronica rilasciata da uno Stato membro, questa verrà riconosciuta anche presso gli altri Stati membri al fine di permettere l'accesso ai servizi online che lo richiedono in modalità transfrontaliera. Il livello di garanzia richiesto è di livello due o tre, salvo la libertà degli organismi del settore pubblico di accettazione del livello uno [2, articolo 6]. Per quanto riguarda invece i livelli di garanzia, questi vengono suddivisi in basso, significativo ed elevato, che in alternativa sono conosciuti anche come livello uno, due e tre. Un livello basso "fornisce un grado di sicurezza limitato", ed è capace di "ridurre il rischio di uso abusivo o alterazione dell'identità"; un livello significativo "fornisce un grado di sicurezza significativo", e per questo potrà "ridurre significativamente il rischio di uso abusivo o alterazione dell'identità"; infine, un livello di garanzia elevato permette "un grado di sicurezza più elevato" rispetto al

livello precedente e ha come fine quello di "impedire l'uso abusivo o l'alterazione dell'identità" [2, articolo 8].

Nella sezione 2 del capo III troviamo invece una parte sugli organismi di vigilanza che devono essere nominati dagli Stati senza vincolo di sede presso gli stessi Stati dove avranno il compito di effettuare attività di vigilanza ex ante ed ex post sui prestatori di servizi fiduciari qualificati (Qualified Trust Service Provider — QTSP) affinché questi rispettino i requisiti del regolamento eIDAS [2, articolo 17]. Gli organismi di vigilanza sono inoltre tenuti a collaborare tra loro [2, articolo 18].

Nella sezione 3 dedicata ai servizi fiduciari qualificati, viene imposto a questi ultimi una verifica da parte di un organismo di valutazione della conformità da effettuare come minimo ogni 24 mesi per appurare il pieno adempimento al regolamento eIDAS [2, articolo 20]. È possibile accedere a una lista, chiamata "elenco di fiducia" che viene stilata dagli Stati e dove si trovano le informazioni sui prestatori di servizi fiduciari qualificati [2, articolo 22].

Un altro importante elemento che si trova nella sezione 4 è quello che riguarda gli effetti giuridici delle firme elettroniche: queste valgono a tutti gli effetti come prove nei procedimenti giudiziali. Inoltre, una firma elettronica qualificata è giuridicamente equivalente negli effetti ad una firma autografa e deve essere riconosciuta da tutti gli Stati membri [2, articolo 25]. Lo stesso si dice tanto per i sigilli elettronici, di cui si ritengono integri i dati e la correttezza dell'origine di questi ultimi in riferimento a sigilli elettronici qualificati [2, articolo 35], come per la validazione temporale elettronica in merito all'accuratezza della data e dell'ora e alla correttezza dei dati cui è legata [2, articolo 41].

Infine, viene stabilito che entro il 1° luglio 2020 venga rivisto il regolamento per adeguarlo eventualmente ai progressi tecnologici, di mercato e agli sviluppi giuridici, mentre ogni quattro anni è necessario stilare una relazione sui progressi raggiunti [2, articolo 49]. Prevedere un riesame ciclico è sintomo di grande consapevolezza della velocità con cui cambia la tecnologia.

All'epoca, eIDAS è stato in qualche modo una rivoluzione che ha posto le basi da cui ha iniziato a fondarsi un quadro comune a tutti gli Stati europei per l'interoperabilità dei sistemi di identificazione digitale.

2.2 Regolamento di esecuzione 2015/1501/EU, regolamento 2016/679/EU e regolamento 2018/1724/EU

A seguito di eIDAS, vi sono stati numerosi regolamenti. Vogliamo ricordare innanzitutto il regolamento 2015/1501/EU che nasce sulla base dell'articolo 12 del regolamento UE n. 910/2014. Infatti, il regolamento 2015/1501 tratta il quadro di interoperabilità in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e si propone di identificare i requisiti tecnici e operativi nel contesto di interoperabilità. Nello specifico, si parla di nodi, gli elementi mediante cui avviene l'interconnessione tra regimi di identificazione elettronica all'interno dell'unione e che sono in grado di comunicare tra loro e trasmettere informazioni garantendo integrità e autenticità dei dati [9, articolo 2, 5 e 7]. I nodi inoltre, al fine di proteggere i dati personali, non sono autorizzati a conservare i dati personali [9, articolo 6]. Sono tuttavia previste delle eccezioni che comprendono l'identificazione del nodo, del messaggio e data e ora del messaggio. Questi dati vengono conservati solo per un determinato periodo di tempo che varia da Stato a Stato e servono a stabilire le dinamiche di scambio in caso di incidente [9, articolo 9]. Infine, negli allegati, viene descritto l'insieme minimo di dati necessari all'identificazione. Per una persona fisica questi comprendono necessariamente nome, cognome, data di nascita e un identificativo univoco stabilito dallo Stato membro, mentre per una persona giuridica troviamo obbligatoriamente la ragione sociale attuale e l'identificativo univoco dato dallo Stato membro [9, allegato].

Per quanto concerne invece il regolamento 2016/679/EU (General Data Protection Regulation — GDPR), questo si occupa più nello specifico della protezione

delle persone fisiche riguardo al trattamento dei dati personali e della libera circolazione di detti dati. La premessa essenziale che porta alla stesura del regolamento è la volontà di proteggere un diritto fondamentale quale la protezione dei dati di carattere personale nel rispetto della Carta dei diritti fondamentali dell'Unione europea e del Trattato sul funzionamento dell'Unione europea (TFUE). Siccome però negli ultimi decenni c'è stata un'impennata nello scambio di dati personali causata dall'evoluzione tecnologica e dalla globalizzazione, è molto importante cercare di trovare delle soluzioni a favore della protezione dei dati, permettendo al tempo stesso la libera circolazione.

La raccolta e il trattamento dei dati personali devono seguire i principi della "minimizzazione dei dati" e della "limitazione delle finalità", che significa evitare di richiedere dati non necessari ai fini prestabiliti e utilizzarli solamente per le finalità pattuite. Secondo invece il principio della "limitazione della conservazione", i dati raccolti saranno mantenuti per un periodo di tempo circoscritto e utile al raggiungimento delle finalità per cui vengono trattati [10, articolo 5]. Altro elemento importante è il consenso dell'interessato al trattamento dei dati personali, senza cui non è possibile procedere. Se il consenso è dato in forma scritta, allora deve essere definito in maniera chiara e deve essere riconoscibile distintamente da eventuali altre parti [10, articoli 6 e 7]. Un ulteriore tratto saliente del regolamento è dato dal "diritto all'oblio" (conosciuto anche come "right to be forgotten"): l'utente può infatti chiedere la cancellazione dei dati che lo riguardano in situazioni circoscritte, ad esempio nei casi in cui non sono più necessari allo svolgimento degli intenti per cui erano stati chiesti, oppure di fronte a trattamento illecito [10, articolo 17]. Inoltre l'interessato può avvalersi del "diritto alla portabilità dei dati", secondo cui può richiedere la trasmissione dei dati a un altro titolare di trattamento [10, articolo 20]. Ciò che rimane come punto fermo è la determinazione nella protezione dei dati, che deve stabilirsi fin dalla progettazione ad esempio mediante pseudonimizzazione dell'interessato [10, articolo 25]. Un altro sistema volto alla protezione dei dati è quello dei meccanismi di certificazione, di sigilli e marchi di protezione, utili alla

dimostrazione di previsione di garanzie adeguate nel rispetto del regolamento [10, articolo 42]. In generale però, le linee guida per la protezione sono costituite dalla pseudonimizzazione e dalla cifratura di dati personali, dal fatto di riuscire a garantire "la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento", dall'idoneità al ripristino immediato della disponibilità e dell'accesso ai dati personali nei casi in cui si verifichino incidenti fisici o tecnici, e infine da "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative" capaci di assicurare fiducia e protezione nel trattamento [10, articolo 32]. Gli standard di sicurezza vengono stabiliti ponderando rischi di trattamento che dipendono dalla "distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati" [10, articolo 32].

Infine passiamo al regolamento 2018/1724/EU attinente all'istituzione di uno sportello digitale unico (EU Single Digital Gateway) per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi. Lo sportello si inserisce nel portale "Your Europe" e permette di accedere a numerose informazioni riguardanti i diritti e gli obblighi legati al mercato interno, procedure in linea e link utili [11, articolo 2]. Inoltre, l'interfaccia utenti deve presentare caratteristiche specifiche, come l'intuitività di utilizzo, l'accesso in linea dai dispositivi elettronici mediante i diversi navigatori di rete e infine deve abbracciare i requisiti di "percepibilità, utilizzabilità, comprensibilità e solidità" durante l'accesso alla rete [11, articolo 18]. Uno degli argomenti essenziali presentati è quello del potenziamento del mercato interno delle procedure in linea e della digitalizzazione rivolto a promuovere la non discriminazione nell'utilizzo dei servizi. Infatti, se una procedura interna a uno Stato può essere esercitata in linea dagli utenti non transfrontalieri, allora questa lo sarà anche per gli utenti transfrontalieri mediante una soluzione tecnica che non deve essere necessariamente la stessa [11, articolo 13]. A questo scopo, è necessario però fornire l'accesso alle informazioni nelle lingue più comprensibili o studiate dai cittadini degli Stati europei [11, articolo 13].

2.3 L'Agenzia dell'Unione europea per la cybersicurezza e il regolamento 2019/881/UE

Il regolamento 2019/881/UE è di particolare interesse perché tratta l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) e anche la certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (Information and Communication Technology — ICT). Nelle premesse si ripetono in un certo qual modo le stesse motivazioni di impegno verso la fiducia nelle soluzioni digitali, necessaria come conseguenza della digitalizzazione, della connettività, e della più recente frontiera dell'Internet degli oggetti (Internet of Things — IoT) che metterà sul campo una quantità consistente di dispositivi digitali connessi. In questo contesto però è indispensabile andare ad incrementare la sfera ancora inadeguata della cybersicurezza, avvalendosi anche delle certificazioni. In particolare, sono in costante aumento gli attacchi informatici, dove buona parte di essi risulta essere di carattere transfrontaliero, e pertanto, arrivare a dei risultati concreti contro questo problema è possibile solo usufruendo del coordinamento tra gli Stati. Inoltre, sarà opportuno attuare misure di "sicurezza fin dalla progettazione" nell'elaborazione di prodotti, servizi e processi ICT per anticipare possibili attacchi informatici e limitare il più possibile gli effetti negativi.

A questo proposito viene sviluppato il progetto ENISA, un'agenzia indipendente istituita già nel 2004 e a cui poi è stato prorogato il mandato nel 2013 con il fine di diffondere e accrescere la cybersicurezza nella Comunità andando a cooperare con università e istituti di ricerca per allargare il bacino di prodotti e servizi utili alla cybersicurezza prodotti in ambito europeo, piuttosto di ricorrere al mercato estero. Alla luce dei cambiamenti avvenuti e dell'evoluzione della politica in materia di cybersicurezza, è risultato opportuno rivedere ed estendere il mandato dell'ENISA a tempo indeterminato.

L'ENISA, oltre a collaborare con gli Stati membri, le istituzioni e gli organismi europei per potenziare la cybersicurezza e diminuire la divisione del mercato interno,

si pone come punto di riferimento a cui chiedere pareri nel campo della cybersicurezza [12, articolo 3]. In tal senso mette a disposizione consulenze di carattere scientifico e tecnico, assistenza, informazioni e migliori pratiche in aiuto degli Stati e delle istituzioni [12, articolo 4]. Tutta l'expertise dell'agenzia viene ricavata specialmente da analisi delle tecnologie emergenti con rispettivi effetti attesi sulla cybersicurezza, e da studi sulle minacce informatiche nel lungo periodo [12, articolo 9]. Sostiene inoltre lo sviluppo di una certificazione unica europea della cybersicurezza, come anche maggiore consapevolezza tra le persone nei riguardi della cybersicurezza mediante l'alfabetizzazione informatica [12, articolo 4 e 8]. Oltre a ciò, ha il compito di appoggiare lo sviluppo dei settori di identificazione elettronica e dei servizi fiduciari [12, articolo 5].

Per svolgere al meglio le sue funzioni di cooperazione ed evitare la duplicazione di attività, stabilisce relazioni con le autorità di vigilanza europee e altre autorità competenti tra cui spiccano il Centro europeo per la lotta alla criminalità informatica (European Cybercrime Centre — EC3) presso Europol, la CERT-UE, il Centro UE di situazione e di intelligence (European Union Intelligence and Situation Centre — EU INTCEN) presso il Servizio europeo per l'azione esterna [12, articolo 7]. Infine, viene costituito un gruppo europeo per la certificazione della cybersicurezza (ECCG), con il compito di supportare e cooperare con l'ENISA e di fornire pareri alla Commissione in materia di certificazione della cybersicurezza [12, articolo 62].

2.4 L'Istituto Europeo per gli Standard nelle Telecomunicazioni (ETSI)

L'Istituto Europeo per gli Standard nelle Telecomunicazioni (European Telecommunications Standards Institute — ETSI) viene istituito nel 1988 dalla Conferenza Europea per le Poste e Telecomunicazioni (CEPT) su volontà della Commissione europea. Viene qualificato come organismo internazionale indipendente e non profit e la sua sede si trova a Sophia-Antipolis in Francia. Insieme

al Comitato europeo di normazione (CEN) e al Comitato Europeo di Elettrotecnica (CENELEC), ETSI è una delle tre organizzazioni riconosciute a livello europeo come produttrice di standard. Il picco di standard emessi accresce notevolmente a ridosso degli ultimi anni, fino a raggiungere quota 40000 nel 2018. Il compito attribuito all'istituto è quello di sviluppare, ratificare e testare non solo standard , ma anche applicazioni e servizi utili e usufruibili in tutto il mondo nel settore ICT. In aggiunta, ricopre la veste di supporto al processo di legislazione europea. Per svolgere al meglio tutte queste funzioni, lavora a stretto contatto con numerosi partner globali, tra cui spiccano ad esempio l'Unione Internazionale delle Telecomunicazioni (ITU) e l'Organizzazione Internazionale per la Standardizzazione (ISO). Ciò permette di allinearsi con gli standard elaborati da altri, di evitare un'inutile duplicazione di sforzi e soprattutto di garantire che il lavoro svolto sia ampiamente accettato e implementato.

La cybersicurezza rientra tra i numerosi ambiti di attività di ETSI; in particolare, vi è un organo interno dedicato chiamato Cybersecurity Technical Committee (TC CYBER) che grazie alla sua expertise offre non solo standard ma anche consigli ai vari utenti attraverso un lavoro a stretto contatto con gli stakeholder. Gli standard così sviluppati mirano ad accrescere sicurezza e privacy a favore dei cittadini e delle organizzazioni in Europa e a livello globale. Il lavoro di TC CYBER si divide principalmente in nove aree tematiche: comprensione dell'ecosistema della cybersicurezza, protezione dei dati personali e delle informazioni, sicurezza dei dispositivi IoT, cybersicurezza delle infrastrutture nazionali di maggiore criticità, cybersicurezza personale, nelle aziende e nelle organizzazioni, supporto a procedimenti legali e criminali, strumenti e tecniche di cybersicurezza, supporto alla legislazione europea e infine crittografia quantum-safe.

Di seguito vengono riportate le norme ETSI più importanti sviluppate per tracciare una linea comune di raccordo alla complessità degli strumenti digitali in materia di identificazione.

ETSI EN 319 401	Requisiti generali per i servizi fiduciari
ETSI EN 319 403	Requisiti per la valutazione di conformità dei servizi fiduciari
ETSI EN 319 411	Requisiti per i servizi fiduciari che emettono certificati
ETSI EN 319 421	Requisiti per i servizi fiduciari che emettono time-stamps
ETSI EN 319 521	Requisiti per i servizi di raccomandata elettronica
ETSI EN 319 531	Requisiti per i servizi di consegna elettronica
ETSI TS 119 431	Requisiti per i servizi fiduciari che forniscono generazione di firme e sigilli
ETSI TS 119 441	Requisiti per i servizi fiduciari che forniscono servizi di validazione
ETSI TS 119 511	Requisiti per i servizi fiduciari che forniscono servizi di preservazione di firme o dati

2.5 L'Organizzazione Internazionale per la Standardizzazione (ISO)

L'Organizzazione Internazionale per la Standardizzazione (ISO) è un'organizzazione indipendente e non governativa con sede a Ginevra in Svizzera e che coopera con la Commissione Elettrotecnica Internazionale (IEC). Ne fanno parte 165 organizzazioni nazionali di standardizzazione dislocate in tutto il mondo, ma con un massimo di un membro per Paese. Fondata nel 1946, ISO negli anni ha prodotto più di 20000 standard riguardanti gran parte degli elementi rilevanti tecnologia e manifattura, con l'intento di fornire formule ideali per realizzare qualcosa a livello comune. Per produrre uno standard, innanzitutto c'è bisogno che il mercato e gli stakeholder esprimano la necessità di una linea guida in un determinato ambito. In seguito, uno standard viene elaborato da un team di esperti nominato dai membri ISO che vota la norma attraverso processi collegiali. Tutto questo iter richiede tempi in media di tre anni.

Le principali norme ISO che contribuiscono a delineare i parametri in materia di sicurezza delle informazioni e di certificazione dei prodotti ICT sono riassunte nella tabella che segue.

Vocabolario	ISO/IEC 27000	Sistemi di gestione della sicurezza delle informazioni: panoramica e vocabolario
Requisiti	ISO/IEC 27001	Certificazione del processo di gestione della sicurezza ICT
	ISO/IEC 27701	Gestione della privacy: requisiti e linee guida
	ISO/IEC 15408	Certificazione del prodotto ICT
Linee guida	ISO/IEC 27002	Codice di condotta per la gestione della sicurezza delle informazioni
	ISO/IEC 27005	Gestione dei rischi per la sicurezza delle informazioni
	ISO/IEC 27014	Governance della sicurezza delle informazioni
	ISO/IEC 27018	Codice di condotta per la protezione delle informazioni di identificazione personale (PII) nei servizi di public cloud per i cloud provider
	ISO/IEC 27034	Gestione della sicurezza nelle applicazioni

CAPITOLO III
La normativa nazionale

Sulla scia dei cambiamenti in atto a livello di Unione europea per un migliore accesso a beni e servizi online in modalità transfrontaliera e per sfruttare il potenziale dell'economia digitale europea, l'Italia non si tira indietro e partecipa a sua volta con normative, piani e iniziative interne. Queste, ancora una volta, non sono interamente il frutto delle evoluzioni degli ultimi anni, ma hanno iniziato a svilupparsi nel corso dell'ultimo ventennio. Quel che è certo è la forte crescita avvenuta nel periodo più recente, da cui ne deriva un boom nella possibilità di usufruire di servizi on-line, con un costante e graduale switch-off al digitale di ciò che rimane ancora disponibile in modalità analogica. Per far fronte alla sfida della trasformazione digitale della Pubblica Amministrazione italiana, è stata creata un'agenzia apposita, l'AgID, con il compito di guidare e supportare questo periodo di transizione. Invece, inerentemente alla digitalizzazione, il testo normativo per eccellenza rimane a oggi il CAD, di cui si parlerà a breve.

3.1 Il Codice dell'amministrazione digitale (CAD)

Il Codice dell'amministrazione digitale (CAD) è un testo unico varato nel 2005 con il decreto legislativo n.82 del 7 marzo, e poi modificato nel 2016 e 2017 con l'intento di concretizzare e appoggiare i diritti di cittadinanza digitale. Data l'importanza del documento per l'informatizzazione della Pubblica Amministrazione e la volontà di coinvolgimento di cittadini e imprese verso servizi sempre più digitali e semplificati, di seguito si delineeranno in maniera sintetica gli aspetti principali e di maggior interesse.

Innanzitutto viene sottolineato il diritto di accesso ai servizi on-line tramite la propria identità digitale [1, articolo 3-bis]. I servizi comunemente erogati in formato analogico devono essere resi disponibili on-line, preoccupandosi della riorganizzazione e aggiornamento dei servizi a scopo di allineamento con le concrete esigenze degli utenti [1, articolo 7].

Per raggiungere tutti gli obiettivi di digitalizzazione e trasferimento dei servizi in modalità on-line, è però imprescindibile sostenere la trasmissione della cultura digitale tra i cittadini con progetti di alfabetizzazione informatica rivolti per lo più ai minori e alle categorie a rischio di esclusione [1, articolo 8]. Oltre a ciò, l'ausilio della tecnologia sarà di notevole aiuto nelle attività di partecipazione dei cittadini alla vita politica, anche per chi non risiede in Italia [1, articolo 9].

Riguardo la pianificazione dell'attività delle Pubbliche Amministrazioni e i rapporti con altre Pubbliche Amministrazioni o privati, questi devono avvenire mediante l'impiego delle tecnologie dell'informazione e della comunicazione, soddisfando in questo modo i principi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione tipici dell'operato amministrativo. Si potrà inoltre migliorare le prestazioni lavorative stimolando l'impiego di dispositivi elettronici personali da parte dei lavoratori [1, articolo 12].

Per poter guidare la trasformazione digitale della Pubblica Amministrazione verso una maggiore semplificazione e crescita, è prevista la figura del Responsabile per la Transizione al Digitale (RTD). In tutte le amministrazioni è obbligatorio individuare un ufficio dedicato con all'interno il RTD, i cui compiti saranno quelli di regolare la transizione al digitale mediante poteri di riorganizzazione, coordinazione e indirizzo. L'obiettivo ultimo del RTD resta quello di ottenere servizi facilmente accessibili e di qualità [1, articolo 17].

Inoltre, non si può dimenticare l'impegno di digitalizzazione rivolto ai documenti detenuti dalla Pubblica Amministrazione: in questo senso sarebbe opportuna una dematerializzazione dei documenti in favore di archivi puramente informatici [1, articolo 42].

Come ultimo elemento da ricordare, vi è la creazione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) che permette l'accesso ai servizi in rete degli utenti che lo richiedono [1, articolo 64].

3.2 L'Agenzia per l'Italia Digitale (AgID)

L'agenzia per l'Italia Digitale (AgID) nasce nel 2012 come agenzia tecnica della Presidenza del Consiglio. All'interno del CAD viene descritta come l'ente avente la missione di attuare le finalità dell'Agenda Digitale Italiana e di quella europea all'interno del contesto di innovazione digitale e dell'impiego delle tecnologie digitali nella Pubblica Amministrazione. I suoi incarichi fondamentali possono essere riassunti nella promulgazione di linee guida, programmazione e coordinamento delle attività delle amministrazioni per l'impiego delle tecnologie dell'informazione e della comunicazione, controllo delle attività svolte, emanazione di pareri tecnici e attività di vigilanza [1, articolo 14-bis]. È inoltre responsabile di approvare o meno la domanda di qualificazione dei soggetti che vogliono fornire servizi fiduciari qualificati e dei soggetti che vogliono prestarsi come gestori di posta elettronica certificata o di identità digitale [1, articolo 29].

Per quanto riguarda le attività di controllo, l'AgID è l'autorità nazionale con il compito di vigilare sui servizi fiduciari, sui gestori di posta elettronica certificata, sui soggetti accreditati che erogano servizi di conservazione e sui soggetti che partecipano a SPID [1, articolo 14-bis]. Se vengono rilevate violazioni, l'AgID è autorizzata ad applicare sanzioni amministrative ai soggetti vigilati tenendo conto dell'entità del danno provocato. Importante risulta anche la rendicontazione: l'agenzia elabora un rapporto nazionale annuo che pubblica sul sito dell'AgID, mentre entro il 31 marzo di ogni anno presenta una relazione alla Commissione europea contente le azioni svolte e le violazioni rilevate [16].

Siccome la componente di salvaguardia dei diritti di cittadini e imprese è fondamentale per l'AgID, viene prevista una figura posta a tutela di questi diritti conosciuta come Difensore civico per il digitale [1, articolo 17]. Le funzioni che ricopre si basano sulla raccolta di segnalazioni riguardanti la violazione delle norme inerenti innovazione e digitalizzazione, oppure si occupa di tutelare i soggetti in merito all'accessibilità agli strumenti informatici [17].

3.3 I piani per l'innovazione e l'informatica nella Pubblica Amministrazione

Per adempiere al suo mandato e far fronte alle novità tecnologiche, l'AgID crea dei piani che si sviluppano nel corso di diversi anni, così da prefiggersi dei propositi ben determinati da realizzare. In particolare, si vuole ricordare il Piano triennale 2019-2021 e 2020-2022 per l'informatica nella Pubblica Amministrazione, e il Piano nazionale innovazione 2025. Nel piano triennale 2019-2021 vengono enunciati dei principi chiave per l'avanzamento della trasformazione digitale della Pubblica Amministrazione. In primo luogo troviamo "digital by default" secondo cui le amministrazioni dovrebbero offrire come modalità predefinita servizi puramente digitali, e "digital identity only" in cui dovrebbe essere promossa la diffusione delle identità digitali. I servizi messi a disposizione dovranno rispettare anche le caratteristiche di inclusività e accessibilità verso le categorie a rischio di esclusione, dovranno tutelare i dati personali degli utenti sin dalla progettazione, e infine essere interoperabili e transfrontalieri per raggiungere le esigenze del mercato unico europeo [18].

Per quanto riguarda invece il Piano nazionale innovazione 2025 si vuole menzionare due tra le 20 azioni illustrate per trasformare il Paese. In primo luogo emerge nuovamente il tema delle identità digitali, con l'obiettivo di raggiungere la totale copertura della popolazione. L'identità digitale deve essere intuitiva, sicura e permettere senza eccezioni l'accesso a tutti i servizi digitali pubblici e privati in Italia

e in Europa. Per servizi si intende praticamente qualsiasi cosa sia accessibile on-line, dalla compilazione della dichiarazione dei redditi all'home banking ad esempio. In aggiunta, nel momento in cui l'utente accede a un servizio, verranno comunicate automaticamente al fornitore due tipologie di informazioni, quali i dati qualificati, come il possesso della patente, e dati non qualificati come un indirizzo email semplice. La seconda azione, nella prospettiva secondo cui tutti avranno un'identità digitale, allora sarà di dotare tutti di un domicilio digitale, vale a dire un indirizzo di posta elettronica certificata. Essere in possesso di un domicilio digitale significa per un cittadino non solo poter semplificare notevolmente la gestione della corrispondenza avente valore legale, ma anche realizzare un notevole risparmio. Lo stesso vale per la Pubblica Amministrazione che sarà agevolata nelle attività di spedizione, ricezione e archiviazione. Per concretizzare questo obiettivo sarà necessario stilare un registro unico dei domicili digitali che ciascun cittadino avrà scelto. È previsto per il futuro l'obbligo di possesso di un domicilio digitale [19].

Infine si arriva al recentissimo Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022, pubblicato a luglio 2020. Il Piano chiaramente si presenta come un'evoluzione rispetto a quelli precedenti, ma questa volta l'attenzione si concentra sul voler coinvolgere attivamente i singoli enti pubblici decentralizzati, che saranno responsabili in prima persona del proseguimento del processo di innovazione tecnologica e trasformazione digitale. Infatti per ogni macro obiettivo viene spiegato esplicitamente alle amministrazioni come devono comportarsi nei prossimi mesi e vengono espressi per punti gli step che devono raggiungere gradualmente. Il catalizzatore dell'innovazione del Paese deve quindi essere necessariamente la Pubblica Amministrazione stessa [20].

Gli obiettivi da perseguire sono sostanzialmente gli stessi emersi nei piani precedenti, ovvero incoraggiare lo sviluppo di una società digitale con al centro cittadini e imprese, sostenere uno sviluppo sostenibile e inclusivo grazie alla digitalizzazione, e infine diffondere ancora di più le tecnologie digitali in ambito pubblico e privato [20].

Per far si che gli utenti privilegino sempre più i canali on-line, i servizi pubblici digitali devono lavorare molto sulla qualità, sul valore e sulla user experience, cercando di privilegiare inclusività, interoperabilità e non frammentazione. In poche parole l'utilizzatore finale deve essere posto al centro in un'ottica di semplificazione estrema. Le amministrazioni da parte loro collaborano e si scambiano software open source per massimizzarne il riuso e quindi le risorse impiegate [20].

Relativamente alle piattaforme, si sottolinea che queste devono essere riusabili e trasversali. Le funzioni offerte dalle piattaforme infatti possono davvero fare la differenza, permettendo di diminuire in modo consistente la mole di lavoro degli uffici e di attuare modalità di risparmio in termini di tempo e denaro. Si punta tutto sul back-office quindi, che deve stimolare la creazione di ulteriori servizi digitali e la semplificazione dei processi. A questo proposito, vanno appoggiate e migliorate le piattaforme già esistenti, e vanno promosse nuove piattaforme, come la recente app IO che dovrebbe consentire l'interazione a tutto tondo del cittadino con la Pubblica Amministrazione e la piattaforma INAD che si propone il compito di gestire l'Indice nazionale dei domicili digitali di chi non è tenuto all'iscrizione presso albi professionali [20].

Particolare attenzione si riversa sulle infrastrutture digitali in ottica di modernizzazione delle Pubbliche Amministrazioni. Le infrastrutture infatti sono il veicolo primario che permette di fornire i servizi, e per farlo non devono solo essere efficienti e sostenibili, ma soprattutto sicure. L'affidabilità e la protezione dei dati personali infatti racchiudono la sfida più importante su cui si basa il lavoro da svolgere sulle ancora numerose infrastrutture digitali pubbliche che mancano dei requisiti di sicurezza adeguati a prevenire attacchi cibernetici. Solo garantendo la sicurezza è possibile ispirare fiducia e quindi aumentare l'utilizzo dei servizi digitali. Inoltre, sarà essenziale evitare la frammentazione infrastrutturale e privilegiare soluzioni condivise e interoperabili. Sempre in ottica di potenziamento infrastrutturale sarà altresì necessario apportare degli aggiornamenti al modello di

connettività per potenziare le prestazioni delle Pubbliche Amministrazioni anche pensando a possibili soluzioni di lavoro agile [20].

Interessante infine lo spunto di riflessione che comporta l'emergenza sanitaria di quest'anno. Ad AgID, in collaborazione con altri soggetti istituzionali, viene chiesto nel corso del prossimo anno di stilare degli studi di fattibilità per una piattaforma in merito allo smart working nella Pubblica Amministrazione e per una piattaforma nazionale di e-learning [20].

3.4 Il documento informatico: nuove linee guida

Come ultimo elemento da riportare relativamente alla normativa interna e alla digitalizzazione della Pubblica Amministrazione, vi è il documento informatico. Innanzitutto vediamo di cosa si tratta e come viene descritto. Secondo il CAD, un documento informatico è un documento elettronico, quindi contrapposto al documento analogico, "che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" [1, articolo 1]. Troviamo invece la definizione di documento elettronico nel Regolamento eIDAS, delineato come "qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva" [2, articolo 3].

Recentemente l'AgID ha elaborato delle nuove linee guida sulla formazione, gestione e conservazione dei documenti informatici per aggiornare le precedenti regole tecniche e riordinare la disciplina raggruppando in un unico documento quanto emerso negli anni in materia di documento informatico. Ancora una volta il fine ultimo risulta essere la semplificazione.

Nella gestione documentale le tre fasi di formazione, gestione e conservazione presentano caratteristiche differenti, e solo una gestione corretta di tutto il processo permette di rispettare i principi propri della gestione archivistica [21].

Relativamente alla formazione di un documento informatico, emergono differenti modalità, dove tutte devono essere accomunate da immodificabilità e integrità, perseguibili ad esempio attraverso una firma elettronica qualificata o avanzata, un sigillo elettronico qualificato, sistemi di gestione documentale sicuri o mediante l'uso di un sistema di conservazione. Forse il metodo più interessante di formazione di un documento informatico, al di là dei più comuni pdf, è quello mediante la compilazione di moduli e formulari on-line, oppure tramite il raggruppamento di un insieme di dati provenienti da una o più banche dati. Anche la certezza dell'autore acquisisce una certa rilevanza, essendo un elemento permanente e certo del documento che permette di legare soggetto e documento stesso. Vi è un caso particolare dato dal documento amministrativo informatico, il quale oltre ai requisiti sopracitati, deve presentare una registrazione in particolare nel registro di protocollo per il tracciamento e la storicizzazione di ogni operazione [21].

Per quanto concerne invece la gestione documentale, ogni Pubblica Amministrazione deve nominare un responsabile alla gestione documentale come figura per il coordinamento delle attività. Inoltre, al fine di ottenere maggiore organizzazione, occorre classificare i documenti amministrativi informatici nella formazione dell'archivio mediante fascicoli informatici o serie documentarie. I formati dei file invece devono avere le caratteristiche di essere indipendenti dai dispositivi, essere formati aperti e non proprietari. Inoltre, tutto il processo di gestione documentale deve coordinarsi con le misure di sicurezza del regolamento europeo sulla protezione dei dati personali e da quanto espresso dall'AgID [21].

Dal sistema di gestione documentale i fascicoli vengono trasferiti al sistema di conservazione che si comporta come un archivio, garantendo quindi l'accesso per il tempo previsto. Non è obbligatorio svolgere i processi di conservazione all'interno dell'ente, ma è possibile usufruire di servizi di esternalizzazione rivolgendosi a conservatori pubblici o privati accreditati presso l'AgID. È inoltre prevista un'altra figura come responsabile della conservazione, funzione che può essere svolta anche dal responsabile della gestione documentale, oppure per le organizzazioni estranee

alla Pubblica Amministrazione, da un soggetto terzo tanto all'organizzazione stessa quanto al conservatore accreditato di cui usufruisce l'organizzazione. Sempre in ambito di conservazione, questa deve avere luogo materialmente sul territorio nazionale [21].

Per concludere, in ambito di digitalizzazione, viene introdotta la "certificazione di processo" che consente di operare una dematerializzazione massiva, attestando l'uguaglianza dei documenti analogici rispetto ai loro corrispondenti digitali durante tutto il processo di dematerializzazione [21].

CAPITOLO IV

Strumenti per l'innovazione e la digitalizzazione in Italia

Per introdurre questo capitolo, ha senso soffermarsi su un particolare indice europeo che raggruppa gli indicatori più rilevanti in merito alle performance digitali, al fine di elaborare un'idea del progresso compiuto verso la competitività digitale. Questo indice è meglio conosciuto come Digital Economy and Society Index (DESI) e consente alla Commissione Europea di effettuare un monitoraggio concreto degli Stati già dal 2014. Gli indicatori su cui viene misurato il risultato sono la connettività, il capitale umano, l'uso dei servizi Internet, l'integrazione delle tecnologie digitali e i servizi pubblici digitali. In base ai dati del 2019, nella classifica DESI 2020 l'Italia si colloca al di sotto della media europea al venticinquesimo posto, con un punteggio di 43.6. Limitatamente alla digitalizzazione della Pubblica Amministrazione, l'offerta di servizi pubblici digitali, anche se piuttosto consistente rimane ancora al di sotto della media europea. Infatti, questi vengono sottoutilizzati a causa dello scarso livello di competenze digitali. Il decollo inoltre è reso difficile anche dal peso delle persone che non hanno mai utilizzato Internet (17%) e dalla poca interazione tra cittadini e Pubblica Amministrazione, dove solo il 32% dei cittadini fa uso di servizi di e-government. Detto questo, i dati però fanno emergere nell'ultimo anno una certa accelerazione nei progetti di amministrazione digitale [24].

In questo capitolo verrà presentata una carrellata di strumenti che rappresentano un input alla digitalizzazione della Pubblica Amministrazione italiana. In primis si descriveranno i diversi sistemi che permettono l'identificazione digitale di un cittadino, e poi si vedranno eventuali ambiti di applicazione interni alla Pubblica Amministrazione e ulteriori progetti legati alla digitalizzazione del Paese. Infine si accennerà a qualche dato sull'avanzamento digitale italiano.

4.1 Sistema Pubblico di Identità Digitale (SPID)

Il Sistema Pubblico di Identità Digitale (SPID) promosso da AgID è operativo dal 2016 e consente attraverso un accesso unico, sicuro e protetto di usufruire dei servizi on-line di Pubbliche Amministrazioni e soggetti privati aderenti mediante l'uso di un'unica Identità Digitale. Dal 10 settembre 2019, SPID permette di accedere anche ai servizi on-line delle Pubbliche Amministrazioni dell'Unione, come da regolamento eIDAS. Quindi, se un servizio estero europeo richiede credenziali di uno specifico livello 2 o 3, allora sarà possibile accedere con credenziali SPID di pari livello. Chiaramente vale anche il viceversa: le amministrazioni italiane devono rendere accessibili i servizi ai cittadini europei che utilizzano identità digitali diverse da SPID, previa notifica di queste ultime all'Unione Europea [25]. Per rendere possibile il riconoscimento transfrontaliero di identità digitali tra stati europei sono necessari dei nodi, infrastrutture informatiche in grado di condurre in modo circolare la comunicazione tra i nodi stessi, e poi tra nodi, service provider e identity provider. In particolare, in Italia, grazie al progetto FICEP (First Italian Crossborder eIDAS Proxy) è stato realizzato il primo "server transfrontaliero italiano" [26].

Come è già stato illustrato, un'identità digitale viene rilasciata da un gestore (identity provider). In Italia gli identity provider accreditati presso AgID sono attualmente nove, e c'è piena libertà di scelta per il cittadino sul gestore a cui rivolgersi. Per richiedere SPID, innanzitutto è necessario essere maggiorenni, avere un indirizzo e-mail, un numero di cellulare, un documento di identità in corso di validità (carta di identità, passaporto o patente) e la tessera sanitaria con il codice fiscale. Questi elementi sono necessari per il riconoscimento della persona, in particolare la tessera sanitaria è utilizzata a supporto del contrasto del furto di identità. Nel momento in cui l'utente sceglie un gestore, può iniziare la procedura di iscrizione al suo sito internet, dove inserirà i dati anagrafici con scansione del documento di riconoscimento e creerà le credenziali di accesso. Il passo successivo per ultimare il rilascio dell'identità SPID è quello del riconoscimento, che può essere

effettuato di persona con Carta d'Identità Elettronica (CIE), Carta Nazionale dei Servizi (CNS), Firma Digitale o tramite webcam da remoto [27].

Analogamente alle identità digitali europee, SPID consente uno standard di sicurezza che si basa su tre livelli, dove il livello 2 appare il più comune per l'accesso alla maggior parte di servizi. Il livello 1 è costruito su un userID e una password da modificare almeno ogni 180 giorni. L'autenticazione a singolo fattore porta con sé un rischio moderato, e per questo è consentito l'utilizzo solamente nei casi con limitate conseguenze negative. Il livello 2 si sviluppa sui precedenti userID e password con l'aggiunta di un ulteriore fattore di autenticazione, quale un codice del tipo "one time password". L'autenticazione a due fattori assicura un alto grado di affidabilità ed è utile nei casi che presentano un rischio ragguardevole. Infine, il livello 3 è modellato quasi sugli stessi elementi del livello 2, eccetto per il fatto che l'ulteriore fattore di autenticazione è basato su certificati digitali con chiavi private conservate su altri dispositivi. Essendo in grado di raggiungere un altissimo grado di affidabilità, quest'ultimo livello è raccomandato per tutti gli usi in cui il rischio di abuso di identità può indurre ad esiti di portata seria e grave [28]. È cura dell'utente scegliere il livello di sicurezza più appropriato al proprio uso personale.

In questa relazione tra utenti e identity provider, chiudono il cerchio le parti facenti affidamento sulla certificazione, che sono costituite dalle Pubbliche Amministrazioni e dai privati. Questi sostanzialmente sono i soggetti che offrono servizi on-line previa identificazione degli utenti e per farlo attuano un canale di comunicazione con gli identity provider. Interessante risulta il fronte ancora agli albori dei privati aderenti: solo undici attualmente hanno deciso di permettere l'accesso ai propri servizi tramite autenticazione SPID. D'altra parte, relativamente ai servizi pubblici, il bacino di possibilità è molto più ampio e in costante crescita: SPID permette di accedere, a titolo esemplificativo, a misure di sostegno come il reddito di cittadinanza, il bonus baby-sitter e il bonus vacanze, a 18app, al sito dell'Agenzia delle Entrate, all'iscrizione a concorsi pubblici e molto altro. Una novità invece sarà lo switch-off all'uso di SPID partire dal 1° ottobre 2020 per l'accesso al sito Inps che

non rilascerà più l'usuale pin. Tutti questi elementi sono l'emblema di un'evoluzione che idealmente porterà all'accesso di qualsiasi servizio on-line tramite l'identità digitale [28].

Recente si rivela la possibilità di richiedere SPID per un uso professionale. In questo caso attraverso un'identità SPID è possibile dimostrare l'effettiva qualità di professionista di una persona fisica e la sua appartenenza a un'organizzazione [25].

La creazione di questo intero sistema comporta necessariamente dei costi. AgID però ha decretato che gli utenti saranno esentati per sempre dal pagamento per i livelli di sicurezza 1 e 2, una strategia che sicuramente favorirà l'incremento del bacino di utenti. Gli identity provider hanno però la facoltà di essere retribuiti per servizi aggiuntivi, come l'autenticazione da remoto. Anche le Pubbliche Amministrazioni usufruiranno di SPID gratuitamente, mentre per i fornitori di servizi privati è previsto che SPID sia a pagamento. I costi vengono definiti in base all'uso ("pay per user") e sono uniformi tra identity provider limitatamente ai servizi base, mentre invece c'è libertà su potenziali servizi extra e sul livello di sicurezza 3 [28].

In conclusione non resta che enunciare i vantaggi. Oltre alla notevole semplificazione data dall'evidente caratteristica che consente l'accesso ai servizi con un'unica identità, SPID ha reso possibile moltiplicare il numero di servizi disponibili on-line direttamente da casa. Oltre a ciò, vi sono benefici anche per i privati che offrono servizi, i quali non avranno più l'onere di conservare i dati personali degli utenti con il rischio di attacchi di furto di identità, e potranno così affidarsi a profili che rispecchiano identità certe, senza il pericolo di incorrere in falsi utenti [28].

4.2 Carta d'Identità Elettronica (CIE)

La Carta d'Identità Elettronica (CIE) è il documento di riconoscimento obbligatorio che sostituisce la precedente carta di identità cartacea e allo stesso tempo costituisce

fonte di autenticazione per servizi on-line. La versione 3.0 di CIE viene emessa a partire dal 2016 dal Ministero dell'Interno in collaborazione con l'Istituto Poligrafico e Zecca dello Stato. Oggi si può richiedere direttamente tramite la web app "Agenda CIE" che semplifica il processo di rilascio, ma solo per i Comuni aderenti: si possono infatti caricare tutti i dati comprensivi di foto direttamente on-line e prendere l'appuntamento in Comune dove vengono richieste le impronte digitali, il pagamento (ci si aspetta che a breve sia reso disponibile on-line mediante PagoPA) e la firma sul consenso alla donazione degli organi. Il processo di rilascio resta disponibile interamente presso gli sportelli comunali per chi non ha dimestichezza con le tecnologie informatiche, ma è indubbiamente vero che Agenda CIE velocizza le operazioni dei funzionari [31].

Fisicamente CIE si presenta come una comoda e duratura carta di policarbonato, sulla cui superficie vengono impressi con una stampante laser la foto, i dati del cittadino e il codice fiscale anche in versione codice a barre. A differenza della carta d'identità cartacea che poteva subire facilmente falsificazioni, CIE ha la caratteristica di essere un documento sicuro, perché utilizza standard di sicurezza e tecniche anticontraffazione all'avanguardia [32]. Nello specifico, l'uso di inchiostri speciali, di ologrammi, del microchip e la produzione centralizzata sono gli elementi che ne aumentano la sicurezza e la protezione dei dati dei titolari contro il furto di identità [31]. Tutti i dati del cittadino, le impronte digitali e le informazioni che consentono l'autenticazione on-line sono custodite internamente nel microchip contactless, il cui contenuto viene firmato digitalmente dal Ministero dell'Interno, così da renderlo inalterabile e difficilmente falsificabile. I dati racchiusi nel microchip, escluse le impronte digitali, possono essere letti con un lettore di smart card contactless o avvicinando la carta a uno smartphone con app Idea del Poligrafico, ma solo per Android con tecnologia NFC (Near Field Communication). Per la lettura delle impronte digitali invece sono necessari permessi speciali concessi solo alla autorità di controllo [33].

Oltre alla funzione di riconoscimento e documento di viaggio riconosciuto nell'area Schengen, CIE è funzionale all'accesso a servizi on-line, ponendosi come identità digitale notificata alla Commissione europea e inserendosi come SPID nel nodo eIDAS. In particolare, nel momento in cui viene fatta richiesta di CIE, nella ricevuta vengono stampate le prime parti dei due codici di sicurezza PIN e PUK. Le parti conclusive dei codici vengono ricevute in un secondo momento in allegato alla busta contenente la CIE. Unendo le due metà del PIN è possibile accedere ai servizi in rete dove appare la dicitura "Entra con CIE". Il codice PUK invece è utilizzato dopo tre tentativi non andati a buon fine di inserimento del PIN, sulla falsa riga di una SIM per cellulari [34]. Verificando in modo sicuro l'identità del cittadino, CIE permette di usufruire dei servizi on-line abilitati delle Pubbliche Amministrazioni e privati aderenti (come per SPID), di effettuare check-in, di sostituire il biglietto nei mezzi di trasporto e agli eventi e infine è utilizzabile come badge di identificazione aziendale in ambito lavorativo perché non facilmente cedibile a terzi. Tuttavia, a oggi non è ben chiaro quali siano i servizi che permettano effettivamente l'accesso con CIE, anche se teoricamente dovrebbe essere equiparata a SPID. Sembra però che CIE potrebbe essere utilizzata per abilitare il livello 3 di SPID, essendo un dispositivo di sicurezza esterno, ma al momento è una funzione non ancora implementata e il dibattito rimane aperto [33].

4.3 Carta Nazionale dei Servizi (CNS)

La Carta Nazionale dei Servizi (CNS) è un'ulteriore strumento di identificazione in rete, anche se poco conosciuto, per accedere ai servizi delle Pubbliche Amministrazioni con autenticazione sicura. Viene distribuita dal 2011 su emissione di Regioni e Camere di commercio, ed è meglio ricordata come la tessera sanitaria che ha impresso il codice fiscale dell'utente. In realtà CNS e tessera sanitaria sono due

facce della stessa medaglia, ma vengono viste da punti di vista diversi rispetto alle possibilità d'uso [35].

Fisicamente si presenta come una smart card contenente un microchip con all'interno i dati identificativi del cittadino. La CNS ha funzionalità che non sono rilevanti solo in ambito sanitario per accedere al fascicolo sanitario elettronico, alle cure mediche e ai farmaci in Italia e in Europa, ma permette anche di firmare digitalmente i documenti e di autenticarsi ai servizi pubblici on-line come ad esempio l'Agenzia delle Entrate, l'Inps e l'Inail [35].

Per usufruire dei servizi ulteriori rispetto a quelli offerti dalla tessera sanitaria, è necessario però attivare la CNS, richiedendo i codici PIN e PUK e dotandosi di un lettore di smart card da collegare al proprio computer. É possibile usufruire dei servizi anche presso gli sportelli pubblici aderenti [35].

4.4 Anagrafe Nazionale Popolazione Residente (ANPR)

Nell'ampio processo di digitalizzazione che investe l'Italia degli ultimi anni, l'Anagrafe Nazionale Popolazione Residente (ANPR) o Anagrafe Unica si configura sostanzialmente come la banca dati unitaria nazionale prevista per farvi convergere le anagrafi comunali della popolazione residente (APR) e l'anagrafe degli italiani residenti all'estero registrati in AIRE [36]. Precedentemente infatti, ciascun comune aveva il suo proprio sistema informatico, e risultava difficile instaurare comunicazioni in primis tra gli enti locali stessi, e poi con i gestori di servizi pubblici e le società a controllo pubblico [18]. Oltre ai dati anagrafici dei cittadini, è stato stabilito che su ANPR vengano inseriti anche i registri di Stato civile e i dati delle liste di leva [36]. Alla luce poi dell'emissione di CIE, la piattaforma ANPR integra i due sistemi permettendo l'interscambio dei dati anagrafici in modo sicuro e certo [37].

La migrazione verso ANPR inizia negli ultimi mesi del 2016, ma a oggi non è ancora stata completata: infatti, molti comuni necessitano di realizzare operazioni di

bonifica di duplicati o errori, e per questo il processo si rivela piuttosto lungo e laborioso, dovendo raggruppare quasi otto mila sistemi di archiviazione distinti. L'utilizzo di ANPR dovrebbe anche favorire la standardizzazione dei comportamenti e delle procedure operative degli operatori comunali, essendo lo strumento che dalla pratica di raggruppamento ed omogenizzazione si propone di razionalizzare la spesa con economie di scala [37e 38].

Non è possibile però descrivere ANPR semplicemente come una banca dati per la circolarità anagrafica nazionale, perché una delle finalità principali per cui è stata realizzata è quella di fornire servizi ai cittadini. La piattaforma infatti permetterà al cittadino di accedere in modalità telematica ai propri dati anagrafici (previa autenticazione con identità digitale) e di ricavare certificati prima disponibili solo presso gli sportelli comunali di residenza [18]. Infine non sarà più necessario informare ciascun ufficio pubblico dei propri dati anagrafici e il processo di cambio residenza sarà reso più semplice [38]. Per ulteriori innovazioni e funzionalità è però fondamentale portare a termine la migrazione [38].

4.5 PagoPA

PagoPA è il sistema standardizzato per i pagamenti elettronici a favore della Pubblica Amministrazione. È attivo dal 2012 su spinta dell'AgID in ottemperanza all'articolo 5 del CAD, mentre dal 2018 la gestione è passata alla Presidenza del Consiglio dei Ministri, che ha voluto farne una vera e propria società per azioni partecipata dallo Stato, PagoPA S.p.A. [18]. Pur essendo previsto dalla legge che le Pubbliche Amministrazioni e le società a controllo pubblico aderissero al sistema pagoPA entro il 31 dicembre 2018, a oggi, dopo svariate proroghe, mancano ancora diverse amministrazioni all'appello, mentre la maggior parte di quelle aderenti non risultano propriamente attive in termini di almeno un pagamento ricevuto. L'obiettivo da raggiungere resta quello di comprendere in pagoPA tutti i pagamenti verso le

Pubbliche Amministrazioni, dove la non realizzazione rappresenta purtroppo un limite al sistema, perché l'esperienza dell'utente è ancora troppo frammentata a seconda dell'ente a cui ci si rivolge. Una possibile soluzione al problema è il recente debutto dall'app "IO" di cui si parlerà più avanti [40 e 41].

La relazione tra i cittadini (o imprese) che eseguono pagamenti e le Pubbliche Amministrazioni (o Gestori di pubblici servizi) è guidata dai Prestatori di Servizi di Pagamento (PSP): questi ricevono il denaro dai cittadini e lo inviano all'ente creditore. È da sottolineare la possibilità di pagamento non solo on-line attraverso il sito dell'ente pubblico, ma anche presso gli sportelli fisici e virtuali di home banking dei PSP. A dialogare allo stesso tempo tra Prestatori di Servizi di Pagamento e Pubbliche Amministrazioni vi è un'infrastruttura tecnologica improntata su alti standard di sicurezza: questo è conosciuto come il Nodo dei Pagamenti [41]. Tutti i pagamenti presentano un codice univoco di identificazione (Identificativo Univoco di Versamento — IUV) che favorisce maggiore tracciabilità e permette di avere la prova che la Pubblica Amministrazione abbia ricevuto il pagamento. Un'altra importante novità è l'eventuale superamento dell'avviso di pagamento cartaceo (che però al momento permane): l'utente può infatti ricevere gli avvisi direttamente sul suo smartphone con SMS, e-mail o notifiche in app. A titolo esemplificativo, pagoPA consente di pagare il bollo dell'auto, le tasse universitarie, le multe e i tributi comunali [41].

Per quanto concerne invece i benefici, i cittadini ne guadagnano sotto diversi aspetti: i costi delle commissioni sono trasparenti e i canali di pagamento vengono aumentati nello spirito di concorrenza; vi è certezza sull'importo da versare, e in caso di variazioni questo viene aggiornato; il processo diventa più facile e veloce perché per pagare basta inserire il codice IUV; il rapporto del cittadino con la Pubblica Amministrazione viene uniformato indipendentemente dalla grandezza dell'ente, come anche le comunicazioni di avviso di pagamento che diventano uguali per tutti [18 e 42]. D'altra parte, la Pubblica Amministrazione, incentivando i pagamenti elettronici, taglia notevolmente i costi legati a transazioni e processo, perché ottiene le

somme versate il giorno lavorativo successivo al pagamento direttamente sul conto corrente dell'ente. Evitare la gestione del contante significa eliminare voci di spesa legate a procedure relative alla gestione e servizi di incasso e ad accordi di riscossione. I doppi pagamenti inoltre vengono evitati, e le insolvenze risultano molto meno comuni [18 e 41].

4.6 Fatturazione elettronica

La fattura elettronica è un documento creato digitalmente in formato XML che sostituisce la fattura cartacea e garantisce integrità e autenticità. Dal 1 gennaio 2019 è stata resa obbligatoria l'emissione di fatture elettroniche tra privati come volano per combattere l'evasione fiscale, e questo ha collocato l'Italia al primo posto in Europa in termini di tempistiche. Al momento quindi, con qualche eccezione, tutte le operazioni, siano esse tra soggetti passivi, verso consumatori finali o verso Pubbliche Amministrazioni, devono avvenire attraverso e-fattura. Emettere fattura cartacea dove è prevista una fattura elettronica significa non aver emesso fattura e quindi incorrere in sanzioni [44].

Per l'emissione, è necessario ricorrere a un supporto informatico, quale un computer, un tablet o uno smartphone. Esistono diversi software, servizi web o app disponibili per l'emissione, alcuni anche gratuiti e forniti dall'Agenzia delle entrate. Durante la compilazione della fattura, vi sono degli elementi comuni da inserire, come il destinatario, il tipo di documento, la data e il numero della fattura, la partita Iva del fornitore e del destinatario o il codice fiscale del cliente. Il destinatario riceve la fattura grazie a un Sistema di Interscambio (SDI), il quale provvede a controllare la correttezza e la veridicità dei dati inseriti ai fini fiscali. Se non riscontra nulla di sospetto, invia la fattura all'indirizzo telematico in formato alfanumerico a sette cifre (codice destinatario) o all'indirizzo PEC del destinatario e recapita una ricevuta di consegna al mittente contenente data e ora di consegna. La stessa copia viene

ricevuta direttamente anche dall'Agenzia delle entrate. Al contrario, se emergono degli errori, il SDI respinge la fattura e invia al mittente una ricevuta di scarto contenente il motivo di rifiuto. Se una fattura non viene inviata attraverso il SDI, allora è ritenuta non emessa. È obbligatorio conservare le fatture elettroniche per dieci anni [45].

I vantaggi, come è immaginabile, sono molteplici, il primo dei quali è evidente nell'ottica di contrasto alle frodi fiscali e di controllo della spesa pubblica. Vi è inoltre una prova dell'emissione, dell'integrità e autenticità della fattura, e sono possibili controlli in tempo reale tra l'Iva dichiarata e versata. Per le imprese significa sicuramente un taglio ai costi di gestione legati alla dematerializzazione della fattura, che non deve essere più stampata, spedita e conservata in un archivio fisico. Gli errori di trascrizione, duplicazione o eventuali smarrimenti sono quasi azzerati, e anzi, reperire i documenti diventa molto più veloce [46].

Infine, relativamente all'ambito pubblico, dal 2018 è stato creato presso AgID uno specifico tavolo tecnico permanente con focus sulla fatturazione elettronica. Questo si occupa dell'aggiornamento e del monitoraggio di corretta applicazione delle regole tecniche e delle modalità applicative, di effettuare valutazioni d'impatto e di racchiudere l'insieme delle iniziative legislative riguardanti fatturazione e appalti pubblici [47].

4.7 "IO" app

La novità più interessante in merito alla strategia di digitalizzazione è il lancio ad aprile 2020 dell'app "IO". Il progetto, come si legge nel già citato Piano Triennale 2019-2021, prende forma a partire dal 2018 per racchiudere in un'unica soluzione la maggior parte dei servizi pubblici digitali e trova fondamento nell'articolo 64-bis del CAD che prevede la formazione di un punto di accesso telematico ai servizi stessi.

Una nota interessante allo sviluppo della piattaforma IO è la modalità usata per raggiungere l'attuale versione. Nei mesi precedenti al lancio, già dal 2019, l'app è stata sperimentata dalla partecipazione attiva di un gruppo di utenti, cosa che ha permesso una valutazione efficace della user experience dei cittadini, delle carenze e dei punti di forza di IO. Oltre a questo, l'app è anche un progetto interamente open source, quindi tutto il materiale è reperibile online da chiunque [48].

Ciò che ha spinto verso la realizzazione di questa piattaforma è sicuramente la determinazione nel potenziamento delle comunicazioni tra cittadino e Pubblica Amministrazione, nella semplificazione dell'accesso, della conoscenza e dell'utilizzo dei servizi pubblici digitali e nel sempre maggior impiego di metodi di pagamento telematici [18].

Il progetto è molto ambizioso: l'app dovrebbe consentire di ricevere avvisi direttamente dalle Pubbliche Amministrazioni, poter effettuare pagamenti attraverso pagoPA integrata, e conservare tutta una serie di documenti come certificati o ricevute. Oltre a questo, l'app consente un'autenticazione forte grazie all'accesso consentito solo con SPID o CIE.

Chiaramente, sarà sempre possibile aggiungere nuove funzionalità a quelle già studiate. I servizi disponibili sono ancora pochi ma destinati ad aumentare, tra cui l'adesione di ACI per il pagamento del bollo auto e dell'emissione dei certificati di proprietà dei veicoli, la richiesta del Bonus Vacanze 2020 e alcuni servizi di comuni di grandi dimensioni. È anche possibile visionare il proprio codice fiscale che viene dematerializzato e reso disponibile in versione digitale in tutti i casi dove può essere necessario mostrare il codice a barre dell'utente. Ora sta alle Pubbliche Amministrazioni aderire a IO app e fare in modo che il progetto possa effettivamente decollare.

4.8 Sanità digitale

Parlare di sanità digitale (o eHealth) significa tracciare un argomento piuttosto vasto in cui le tecnologie ICT vengono sfruttate in ambito sanitario per fornire un servizio migliore a tutela della salute dei cittadini e allo stesso tempo ridurre i costi in linea con la sostenibilità del Servizio Sanitario Nazionale.

In questi anni sono numerose le misure prese a favore della sanità digitale, la prima delle quali in ordine di importanza è il Fascicolo sanitario elettronico (FSE), strumento che si propone di comprendere al suo interno la storia sanitaria di tutta la vita dell'utente, permettendo la consultazione in diverse situazioni senza la necessità di corrispettivi cartacei. Non solo il cittadino può accedervi con SPID (o con CNS) dovunque si trovi, ma anche i medici possono consultarlo, previa autorizzazione del paziente, su tutto il territorio, indipendentemente dalla regione di appartenenza dell'utente. È uno strumento estremamente completo, anche alla luce dei casi più urgenti, perché racchiude tutte le informazioni sanitarie e i documenti digitali che riguardano il paziente, senza tralasciare nulla [51].

Vi sono ulteriori elementi a favore di questa linea, come ad esempio il Centro unico di prenotazione (CUP), che centralizzando il sistema di prenotazione delle prestazioni sanitarie, permette di ottenere una consistente diminuzione nei tempi d'attesa. Seguono poi i servizi di telemedicina che si prestano a supporto di una nuova forma di assistenza domiciliare a distanza e per il monitoraggio dei pazienti a rischio, e infine la ricetta elettronica (o ePrescription) che consente al cittadino di usufruire di prestazioni farmaceutiche e ambulatoriali su tutto il territorio [52].

Tra i benefici dell'eHealth emergono come ci si aspetta un consistente tornaconto in efficienza, riduzione dei costi e razionalizzazione delle prestazioni erogate. Inoltre, grazie alla quantità di informazioni a disposizione per ciascun paziente, è possibile limitare gli errori medici, migliorare la gestione della salute dei pazienti stessi, in particolar modo di quelli soggetti a malattie croniche [53].

4.9 Cloud della PA

Il Piano Triennale dell'AgID per l'Informatica 2019-2021 prevede l'attivazione di un'infrastruttura informatica di cloud computing per la Pubblica Amministrazione. L'intuizione legata all'uso del cloud sfrutta la velocità nell'erogazione di servizi grazie alla disponibilità di un gruppo di risorse di calcolo raggiungibili mediante Internet. In questo contesto spariscono le infrastrutture fisiche per lasciare spazio a servizi virtuali il cui costo è determinato in base al consumo. Per far fronte ad adeguati standard di sicurezza, efficienza ed affidabilità, AgID ha studiato un iter per i soggetti interessati a offrire servizi cloud indirizzati alla Pubblica Amministrazione, i cui servizi, se ritenuti conformi ai requisiti, vengono ammessi al Catalogo dei servizi Cloud per la PA [57].

I servizi cloud in generale si presentano sotto forma di tre categorie. Innanzitutto, i software-as-a-service (SaaS) raggruppano tutte le applicazioni software raggiungibili con Internet. Si parla poi di platform-as-a-service (PaaS) in riferimento alle piattaforme utili allo sviluppo e distribuzione delle applicazioni. Infine vi sono le infrastructure-as-a-service (IaaS) che costituiscono l'infrastruttura tecnologica fisica e virtuale dei servizi cloud. In particolare, la Pubblica Amministrazione deve rifarsi al principio di "Cloud First", secondo cui è necessario servirsi essenzialmente delle categorie SaaS, PaaS e IaaS in merito a soluzioni cloud prima di trovare altre alternative tecnologiche [58].

Le motivazioni che spingono verso l'utilizzo del cloud sono prima di tutto di carattere economico e innovativo: usufruire di applicazioni cloud (SaaS) significa minimizzare i rischi, in quanto si investe poco all'inizio in base alle necessità, si paga in base al consumo e non è necessario quindi investire in risorse hardware locali molto costose. Pertanto, nel momento in cui non si usufruisce più di un servizio, questo cessa di essere un costo, ed è possibile dirigersi verso soluzioni diverse con estrema facilità. In secondo luogo, l'uso del cloud pubblico consente di garantire servizi sempre aggiornati e all'avanguardia senza costi aggiuntivi. In aggiunta, questi

servizi sono considerati "user-friendly" per il fatto che sono accessibili tramite Internet utilizzando diverse tipologie di dispositivi. Infine, riguardo privacy e sicurezza, il carico di lavoro della Pubblica Amministrazione viene alleggerito perché non si deve più occupare direttamente di infrastrutture fisiche e software [58].

4.10 Public e-Procurement

Il processo di approvvigionamento di beni e servizi da parte delle Pubbliche Amministrazioni è chiamato Public Procurement. Si parla però di Public e-Procurement se questo processo viene digitalizzato, dove le procedure di aggiudicazione e gestione dei contratti pubblici si devono rifare ai principi di semplificazione, trasparenza, standardizzazione e razionalizzazione della spesa pubblica, tutti elementi fortemente voluti da parte della Commissione Europea. A questo scopo ai processi di approvvigionamento pubblico vengono associati strumenti ICT a supporto delle difficoltà nella gestione degli appalti, che altrimenti possono essere soggetti a realizzare perdite di produttività ed efficienza [62].

Il raggiungimento di questo obiettivo è profondamente complesso per la numerosità di fasi e attori coinvolti. L'idea è quella di riuscire a digitalizzare l'approvvigionamento in toto, quindi partendo dalla fase di pre aggiudicazione, fino ad arrivare allo stadio conclusivo con il post aggiudicazione. Andando al fulcro della questione, il processo di approvvigionamento e quindi di gara avverrà in modalità telematica: citando alcuni degli elementi, i bandi e i documenti di gara saranno in formato elettronico, le offerte di gara saranno accettate solo se giunte in modalità telematica, le fatture e i pagamenti saranno entrambi elettronici [63].

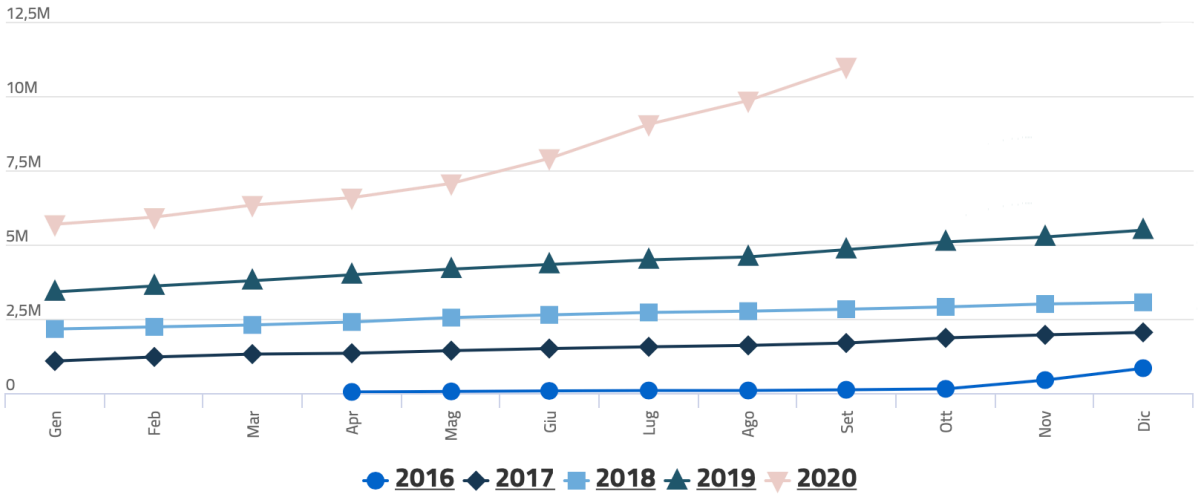
Uno degli elementi da tenere in considerazione è la compilazione del Documento di gara unico europeo elettronico (eDGUE) utilizzato come una sorta di prova alla partecipazione in una procedura d'appalto. Il documento dovrebbe anche favorire l'interoperabilità di partecipazione nel contesto del mercato unico [62].

Tra le altre novità, vi è la Banca Dati degli Operatori Economici (BDOE), che serve ad acquisire e provare il possesso dei requisiti di carattere generale, tecnico-professionale, economico e finanziario ai fini della partecipazione alle procedure di affidamento [62].

Infine, la Commissione Europea ha spinto per la creazione di un progetto pilota per gli appalti elettronici a livello europeo. Questo viene chiamato PEPPOL (Pan-European public Procurement On-Line) e ha il compito di determinare gli elementi infrastrutturali e le specifiche tecniche per favorire la diffusione di procedure di e-Procurement [62].

4.11 Avanzamento della trasformazione digitale in numeri (ottobre 2020)

Dopo aver descritto gli strumenti ideati per attuare la trasformazione digitale, è opportuno dare uno sguardo anche ai dati effettivi di questo avanzamento, per capire la portata e la velocità della trasformazione, e gli eventuali fattori che potrebbero aver influito nella recente accelerazione.



Andamento identità SPID erogate [67]

Partendo da SPID, è piuttosto evidente dal grafico il forte incremento di identità rilasciate negli ultimi mesi a fronte dell'emergenza sanitaria. Il numero di identità SPID raggiunge più di 11 milioni di utenti, un numero importante se si prende in considerazione il fatto che a inizio anno le identità erano la metà (5.5 milioni). Il numero di gestori di identità digitale è nove, tra cui spicca Poste Italiane che ha rilasciato circa l'80% delle identità. Il numero di Pubbliche Amministrazioni che ha abilitato l'accesso ai servizi on-line con SPID è però tuttora abbastanza ristretto (4.478) se comparato al target di 10.000 di quest'anno, cosa che potrebbe costituire un handicap al decollo di questo importante strumento di digitalizzazione. Il numero di privati che offrono servizi on-line accedendo con SPID è di 11, un dato ancora molto basso ma con ampio margine di miglioramento nei prossimi anni [67].

Per quanto riguarda CIE, il numero di cittadini in possesso della carta raggiunge oltre i 16 milioni (28% della popolazione). La percentuale di popolazione che può richiedere CIE è del 94.55% perché alcuni comuni devono ancora adeguarsi all'emissione della carta, mentre gran parte dei comuni si è adeguata nel corso del 2018. Ad Agenda CIE invece, novità di quest'anno, hanno aderito per il momento poco meno del 10% dei comuni [68]. I comuni invece che hanno fatto il subentro ad ANPR sono quasi 6 mila e mezzo, per una popolazione totale presente nella banca dati di più di 47 milioni [69].

Al progetto pagoPA hanno aderito circa l'80% (18.147) delle Pubbliche Amministrazioni e gestori di pubblici servizi. Tuttavia questo non rappresenta un dato effettivo, perché la situazione non è così rosea. Infatti, le Pubbliche Amministrazioni che hanno portato a termine la procedura di attivazione e risultano quindi operative sono l'86,2% (15.660) di chi ha solo aderito. Ancora verso una linea peggiorativa risulta il numero di enti presso cui è andato a buon fine almeno un pagamento, che è di 4.542 (29,1% degli enti attivi), un dato bassissimo se si pensa alla portata innovativa che costituisce la piattaforma [70]. Il dato positivo invece è che le transazioni sono in costante crescita, con un incremento sull'anno dell'86% rispetto a due anni fa [71].

Successivamente, le Regioni in cui risultata implementato e attivo il fascicolo sanitario elettronico sono 14, su un obiettivo di copertura totale per fine 2020, mentre le Regioni aderenti all'interoperabilità delle piattaforme su scala nazionale sono per ora solo 12, sempre su un target di 20 per fine 2020. Il dato peggiore però è quello del numero di cittadini che hanno attivato il FSE: solo il 23% degli assistiti dal sistema sanitario ha aderito, un numero già in ritardo sul target del 25% del 2018 [72].

L'app IO invece è stata scaricata da più di tre milioni e mezzo di persone da giugno 2020 e gli accessi risultano per la quasi totalità effettuati mediante identificazione SPID rispetto a CIE [73]. Il download invogliato dalla possibilità di chiedere il bonus vacanze ha sicuramente aiutato, ma sarà necessario usare qualche ulteriore strategia di attrazione o stimolo nei prossimi mesi per aumentare la fetta di utenti.

CAPITOLO V
I progetti europei

Il rapporto con una tecnologia in costante evoluzione porta sicuramente benefici, tra cui un miglioramento della vita dei cittadini, ma non si possono negare le necessità di ottimizzare i sistemi esistenti e di affrontare tutte le nuove tipologie di rischio, soprattuto in termini di tutela della privacy e protezione dei dati personali. Ciò non significa che i supporti di tipo tecnologico debbano essere eliminati, piuttosto al contrario è necessario trovare soluzioni e indirizzi comuni. Tuttavia per farlo sono necessarie risorse monetarie non indifferenti. A questo proposito, la promozione di studi in Europa è molto consistente e i progetti finanziati con i fondi comunitari offrono importanti e stimolanti proposte e sfide in merito ai diversi ambiti di implementazione dei nuovi strumenti digitali. In questa sezione allora vengono presentati alcuni progetti europei di interesse che si focalizzano su tre principali temi, delineando eventuali progetti pilota e alcune best practices da cui poter prendere spunto: questi progetti riguardano l'interoperabilità, il principio once-only e la protezione dei dati personali.

5.1 I progetti STORK e STORK 2.0

STORK, il cui nome per esteso è Secure idenTity acrOss boRders linKed, è un progetto europeo del periodo 2008-2011 e a cui partecipano numerosi Stati membri nell'ottica di attuazione del mercato unico digitale europeo. È cofinanziato dalla Commissione Europea attingendo al progetto CIP (Competitiveness and Innovation Framework Programme). Il successo è talmente grande che si opta per un secondo progetto STORK 2.0 nel periodo 2012-2015 che si concentra per lo più su una convergenza dei settori pubblico e privato in ambito di eID e sull'identificazione di

persone legali. Nel periodo in cui viene lanciato il progetto esistevano già diverse identità elettroniche rilasciate dai paesi membri, ma mancava il riconoscimento reciproco tra queste diverse identità nazionali. STORK allora si propone di creare uno schema di interoperabilità transfrontaliera per l'utilizzo delle eID senza imporre nessuna soluzione specifica. Infatti, un elemento essenziale del progetto è l'idea di non intervenire nella modifica dei sistemi nazionali, in quanto risultava impossibile, a fronte della quantità enorme di risorse investite, andare ad intaccare sistemi funzionanti già da anni. Vengono previsti allora tutta una serie di progetti pilota riguardanti i servizi più utili ai cittadini europei che sono in seguito testati da un gruppo di Stati aderenti. STORK si rivela per i temi esposti e i problemi sollevati un progetto essenziale e stimolante che pone poi le basi per il regolamento eIDAS del 2014.

In breve, gli obiettivi edificanti del progetto STORK sono capire come interfacciarsi ai problemi di ordine legale e pratico legati alle identità digitali, studiare e implementare delle soluzioni tecniche per sfruttare in modo transfrontaliero le eID, e infine darne prova mediante sei progetti pilota calati in attività tangibili per i cittadini, per provare se quanto emerso dagli studi può funzionare in un contesto reale o meno [74].

Relativamente ai problemi di ordine legale e pratico, questi si possono dividere in tre macro blocchi. Innanzitutto si parla di identificatori personali: l'uso degli identificatori varia da Paese a Paese ed è importante per la gestione delle identità dei cittadini. La legislazione in merito chiaramente è varia, e in molti casi si presentano restrizioni anche nell'uso transfrontaliero. Un ulteriore punto importante emerge sul tema della protezione dei dati. Questi sono tutelati da numerose leggi nazionali, ma è difficile che vengano coperti tutti gli ambiti coinvolti. Per questo, in un contesto di interoperabilità, si propone di coinvolgere attivamente gli utenti, a cui verrà chiesto di volta in volta il consenso al trattamento di specifici dati personali, mostrando allo stesso tempo anche a chi verranno comunicati i dati. Infine, a fronte delle diverse modalità di implementazione nei Paesi europei, è importante capire in

base a quali caratteristiche un sistema di identificazione possa essere definito sicuro. Si parla allora dei famosi livelli di sicurezza: STORK ne prevede addirittura quattro (contro i tre attuali), con un'evoluzione che va dal classico sistema username-password, alle smart card, fino ad arrivare ai certificati qualificati. Si sottolinea che è il fornitore di servizi a decidere a quale livello ammette l'identificazione tramite eID in base alla natura dei servizi stessi [74].

Sull'interoperabilità invece si individuano due strade: il "modello middleware" e il "modello proxy". Secondo quest'ultima soluzione, l'autenticazione è delegata a un'entità esterna, e quindi le interazioni tra service provider e utenti esteri sono gestite da server proxy nazionali (Pan-European Proxy Service — PEPS). Ogni stato membro può avere un solo proxy per gestire i processi di autenticazione transfrontalieri. La peculiarità sta proprio nel fatto che un proxy comunica solo con un altro proxy, oppure con utenti, service provider o identity provider interni allo Stato a cui appartiene. Siccome hanno la responsabilità di gestire i dati almeno nel momento di autenticazione, questi nodi-proxy devono rispettare elevati standard di sicurezza al fine di instaurare condizioni di fiducia tra i punti interessati. Dall'altra parte, l'approccio middleware prevede un'interazione diretta tra utente e fornitore di servizi senza la condivisone di dati con intermediari, per cui il cittadino titolare di eID può direttamente autenticarsi presso un service provider evitando di trasferire prima i dati a una terza parte. Vi è sostanzialmente lo stesso procedimento che avviene tra service provider e un qualsiasi utente interno allo Stato. Questo significa che il fornitore di servizi è responsabile in generale e dal punto di vista della protezione dei dati dell'utente. Lo svantaggio è che il service provider deve dotarsi di strumenti software che riconoscano a tutti gli effetti il cittadino che si autentica con eID straniera. Lo scenario previsto da STORK per raggiungere l'obiettivo di interoperabilità è dato dalla coesistenza dei due modelli, perché ciascuno Stato è libero di utilizzare uno dei casi proposti in base alle valutazioni su fattibilità, livello di protezione dei dati, sicurezza e scalabilità. A questo proposito però viene introdotto un terzo componente, una sorta di identity provider virtuale (V-IDP), con

il compito di mediare tra i due diversi sistemi di gestione middleware e proxy. Questo, in un Paese che ha adottato la modalità middleware, si colloca presso un service provider oppure al livello di comunicazione con il proxy straniero [74 e 75].

Per quanto riguarda i progetti pilota, se ne evidenziano sei tutti accomunati dall'autenticazione dell'utente con eID: "Cross-border Authentication Platform for Electronic Services" punta all'applicazione del paradigma STORK ai servizi di e-government stimolando l'autenticazione con eID dei cittadini; "Safer Chat" riguarda una sperimentazione tra scuole di comunicazione sicura, dove l'accesso degli studenti viene ammesso in base al soddisfacimento di un livello di età verificata con l'autenticazione; "Student Mobility" è pensato per testare l'accesso a servizi di gestione universitari all'estero, come ad esempio la pre-iscrizione da remoto; "Electronic Delivery" vuole provare a sfruttare l'eID all'interno della consegna qualificata transfrontaliera, usando la funzionalità della firma qualificata presente in diverse smart-card europee per la firma della ricevuta; "Change of Adress" facilita i trasferimenti oltre confine trasmettendo il nuovo indirizzo a diverse autorità e coinvolge i provider di attributi (che possono essere distinti dagli identity provider), perché oltre ai dati di autenticazione, vengono comunicati anche quelli del nuovo indirizzo; infine "A2A Services and ECAS integration" vuole unire la già funzionante piattaforma di comunicazione ECAS con il progetto pilota di comunicazione tra amministrazioni mediante identità elettroniche [75].

STORK 2.0 invece presenta quattro progetti pilota calati nella vita reale: "eAcademia", continuando sulla strada del precedente progetto, consente di provare il possesso di attributi accademici per diversi fini e amplia le piattaforme di eLearning; "eBanking" permette a una persona fisica o con un mandato di aprire un conto bancario all'estero e di accedervi on-line; "eGov4Business" propone alle imprese europee di usufruire di servizi pubblici on-line per la registrazione di imprese o l'accesso a portali per le imprese; "eHealth" difende il diritto alla salute consentendo l'acceso alle cartelle cliniche oltre frontiera [76 e 77].

Riguardo le opinioni rilevate dai questionari compilati dagli utenti, emerge nella maggior parte dei casi un giudizio positivo sulla user experience. Lo stesso vale per la valutazione sulla fruibilità, in quanto l'utilizzo di STORK ha permesso in generale di risparmiare tempo (anche nell'ordine di giorni), oppure ha addirittura consentito l'accesso a servizi che altrimenti non sarebbero stati raggiungibili. Infine, relativamente agli indicatori di privacy e sicurezza, pur ottenendo buoni risultati, questi sembrano influenzati dalla percezione dell'utente verso un determinato servizio. Ad esempio, l'ambito dell'eBanking è stato sentito come meno sicuro rispetto agli altri [77].

La conclusione a cui portano tutti questi progetti pilota, per la numerosità di Stati aderenti e le diverse tipologie di identità elettroniche, è che tecnicamente una collaborazione transfrontaliera è pienamente fattibile e può funzionare. Gli elementi che però mancavano ancora erano una base legislativa comune e il riconoscimento reciproco, cosa che poi avviene in via obbligatoria per tutti gli Stati membri a partire dal 2018 su applicazione del regolamento eIDAS. Da STORK 2.0 invece emergono situazioni complesse nella gestione dei mandati, proprio per la difficoltà nella definizione di questa ampia categoria. Tuttavia, è altrettanto vero che l'accesso delle persone legali al bacino di utenti offre una grande possibilità di progettazione di ulteriori servizi. Infine, è stato importante anche il contributo dato dai settori non pubblici, cosa che ha esteso il programma verso utilizzi e sfide che prima non erano stati presi in considerazione [77].

5.2 Due progetti sul principio once-only: TOOP e SCOOP4C

Si è già parlato precedentemente del principio once-only (once-only principle — OOP) secondo cui si ritiene più oneroso chiedere più volte degli stessi documenti rispetto ad effettuare uno scambio di documenti già presenti negli archivi di altre amministrazioni. In breve questo prevede che le Pubbliche Amministrazioni possano

richiedere dei documenti a cittadini e imprese solamente una volta. Dal momento in cui entrano in possesso di determinati dati, se questi sono necessari ad altre amministrazioni, allora occorre che venga attuato uno scambio e un riutilizzo anche transfrontaliero dei documenti tra amministrazioni, in conformità con le norme in materia di protezione dei dati. Risulta pertanto un importante traguardo da realizzare sul fronte della digitalizzazione. I benefici che si ricavano dal OOP sono il risparmio di denaro e quindi di tempo, la riduzione della mole di lavoro in capo alle amministrazioni, lo svolgimento più veloce di obblighi di ordine legale e infine il potenziamento della qualità e dell'efficienza amministrativa. In Stati come Estonia, Paesi Bassi e Belgio il OOP viene già attuato e in molti casi la sua applicazione è stata resa obbligatoria. Tuttavia, se all'interno degli Stati c'è qualche sperimentazione a riguardo, l'implementazione transfrontaliera è considerevolmente ridotta. A questo proposito, la Commissione Europea sta promuovendo il OOP tra gli Stati membri, essendo questo uno dei principi dell'eGovernment Action Plan 2016-2020 europeo e uno degli elementi per la realizzazione del mercato digitale unico europeo. I progetti europei che prendono in esame il OOP sono essenzialmente due: se TOOP si concentra sullo scambio di documenti tra amministrazioni e imprese secondo il OOP, SCOOP4C studia lo stesso tema ma in rapporto al cittadino [81 e 82].

Il progetto TOOP (The Once-Only Principle Project) inizia nel 2017 ed è finanziato all'interno del programma europeo Horizon 2020. Vi partecipano più di venti Stati europei, e la sua conclusione, dopo un'estensione, è prevista per il 2021. Il focus è la riduzione dell'onere amministrativo in capo a imprese ed amministrazioni in merito ad attività commerciali transfrontaliere. Oltre ai progetti pilota calati in situazioni reali per dimostrare la fattibilità e l'utilità del OOP, il programma studia lo sviluppo di una struttura tecnica federata in grado di connettere gli archivi delle amministrazioni europee mediante sistemi ed elementi già esistenti. Inoltre si cerca di assimilare le opinioni provenienti dagli stakeholders e di individuare eventuali punti di criticità. All'interno del progetto, è stato importante anche il rapporto con la

Commissione Europea in merito al regolamento sul Single Digital Gateway del 2018 [81 e 83].

Le principali barriere si evidenziano limitatamente all'ambito legale. È infatti complesso, per l'eterogeneità dei sistemi coinvolti, capire in base a cosa stabilire la validità legale di un documento potenzialmente scambiabile. Teoricamente il problema si risolve: se lo scambio avviene tra archivi, questi sono tenuti a conservare solo documenti validi ed aggiornati. Allo stesso tempo emergono dei dubbi anche riguardo la privacy e la protezione dei dati, ma soprattutto verso la disponibilità delle amministrazioni di adeguarsi a un cambiamento a livello tecnologico. Oltretutto, bisogna capire come superare la barriera linguistica: non tutti gli Stati infatti accettano documenti redatti in lingua straniera e richiedono pertanto delle traduzioni. Un ultimo elemento che vale la pena menzionare è la poca chiarezza sul numero effettivo di utenti finali che potrebbero essere coinvolti dal OOP, cosa che frena sensibilmente l'interesse degli Stati verso questa modalità di acquisizione dei documenti [83].

I programmi pilota sono tre e si qualificano come parte integrante del progetto TOOP dal momento che si configurano come un ambiente ricco di stimoli per l'apprendimento volto agli obiettivi di e-Government. Il primo, "Cross-border e-Services for Business Mobility", mira a facilitare la mobilità delle imprese all'interno dell'unione e la partecipazione ad appalti pubblici, utilizzando lo scambio di informazioni tra amministrazioni dal Paese di origine a quello di destinazione dell'impresa. Ad esempio, un'impresa di un Paese A vuole aprire una filiale in un Paese membro B. L'impresa fa richiesta on-line all'amministrazione competente del Paese B, la quale a sua volta comunica direttamente con l'autorità del Paese A per la trasmissione dei documenti richiesti. Una volta ricevuto il materiale, l'amministrazione di B completa la procedura di registrazione e informa l'impresa [82 e 83].

Poi vi è il pilot "Updating Connected Company Data": per le imprese che operano all'estero in più Stati membri è difficile far pervenire a tutti gli enti che lo

richiedono eventuali dati e aggiornamenti sui documenti d'impresa. Per questo, TOOP ha pensato di creare un sistema che permetta di accedere ai dati dei registri d'impresa nazionali da parte degli enti che lo richiedono. Questo mira ad alleggerire l'intero processo in capo alle amministrazioni e alle imprese, e a ridurre la possibilità di frodi perché possono essere individuate più facilmente rilevando informazioni contraddittorie o inesatte [83].

Infine vi è il programma "Online Ship and Crew Certificates", che prevede l'eliminazione della documentazione cartacea che il capitano doveva presentare al personale di controllo dei porti. Questo processo viene sostituito dallo scambio dei certificati necessari direttamente tra le varie autorità marittime nazionali e offre la possibilità di usare certificati on-line. Il risultato è rilevante per il risparmio di tempo nel controllo dei certificati della nave e dello staff, e per la digitalizzazione di un processo che prima avveniva in formato cartaceo. Inoltre, saranno ridotti eventuali errori o tentativi di frodi in quanto i certificati con dati non corretti verranno scartati in modo automatico. Un freno a questo progetto potrebbe essere rappresentato dalla natura globale del settore navale dei trasporti, e per questo potrebbe risultare non immediato rilevare gli effetti sperati se il sistema non venisse adottato anche da Paesi extra-europei [82 e 83].

Il secondo progetto in merito al OOP è SCOOP4C (Stakeholder Community Once-Only Principle For Citizens) finanziato sempre dalla Commissione Europea con il programma Horizon 2020 nel periodo 2016-2019. Il focus questa volta però non è sulle imprese, ma sul rapporto cittadino-amministrazione. L'obiettivo è capire come riuscire ad implementare il OOP su scala europea a favore dei cittadini, discutendo su possibili dinamiche di co-creazione e co-produzione dei servizi pubblici. In particolare, il progetto prevede l'istituzione di un gruppo di stakeholder come punto centrale per il dibattito e la condivisione di opinioni. Inoltre, vengono presi in considerazione esempi virtuosi di implementazione del OOP e analizzati gli approcci e le soluzioni messi sul campo [84].

Uno dei progetti virtuosi presi in esame è il Birth Registration and Family Allowance (ALF) attivo dal 2015 in Austria. Si tratta di un sistema che permette ai neo genitori di ricevere gli assegni familiari che gli spettano senza dover affrontare un difficile iter burocratico. Sostanzialmente è necessario recarsi solamente all'ufficio di stato civile comunale e presentare un documento di riconoscimento: non c'è bisogno di ulteriore documentazione, perché questa viene automaticamente condivisa dall'ospedale con nove Pubbliche Amministrazioni, previa autorizzazione dei genitori. Tra i servizi a cui si accede con la condivisione dei dati, vi è anche la spedizione della tessera sanitaria direttamente all'indirizzo dei genitori [84].

Gli scenari che secondo lo studio potrebbero essere tra i più apprezzabili sotto il punto di vista del OOP sono diversi: la possibilità di facilitare la mobilità nel settore dell'istruzione negli Stati membri; la protezione sociale in merito ai diritti e doveri delle famiglie coinvolte in situazioni oltre frontiera; la gestione della tassazione in più Paesi per chi lavora temporaneamente all'estero; il trasferimento di un veicolo in modalità temporanea o permanente verso un altro Stato europeo; e infine la sanità, dove si dovrebbe facilitare l'accesso all'acquisto di medicinali prescritti in un altro Paese [84].

Come per TOOP, le barriere alla realizzazione del progetto sono sostanzialmente le stesse. Queste si raggruppano nella mancanza del coinvolgimento politico verso il OOP, nella difficoltà di creazione di un sistema sicuro di scambio dei documenti rispettando i diritti di protezione dei dati dei cittadini europei, nella non omogeneità delle caratteristiche dei documenti nei diversi Stati e infine nella necessità di un meccanismo di trasparenza che permetta al cittadino di verificare quando e per quale motivo un'amministrazione ha fatto utilizzo dei suoi dati personali [85].

5.3 Sfide sulla protezione dei dati personali: PoSeID-on

Tra gli elementi di criticità evidenziati più volte, si è parlato dell'incertezza in merito alla sicurezza data dall'uso di tecnologie in costante evoluzione. Ormai non si può ignorare il fatto che privacy e protezione dei dati personali (Personal Identifiable Information — PII) siano due diritti di fondamentale importanza per i cittadini. Questi diritti hanno radici più lontane di ciò che si potrebbe comunemente immaginare: compaiono infatti nella Dichiarazione Universale dei Diritti dell'Uomo del 1948 (articolo 12), nella Convenzione Europea dei Diritti dell'Uomo del 1950 (articolo 8) e nella Carta dei Diritti Fondamentali dell'Unione Europea del 2000 (articoli 7 e 8). Più recentemente invece viene approvato il General Data Protection Regulation (GDPR) con lo scopo di uniformare la materia a livello europeo e di gestire uno scenario che aveva subito cambiamenti repentini dovuti alla sempre maggiore diffusione delle nuove tecnologie [95].

A questo proposito nel 2018 si inserisce il progetto PoSeID-on (Protection and control of Secured Information by means of a privacy enhanced Dashboard) per supportare l'implementazione diffusa del GDPR e studiare la gestione dei problemi di sicurezza legati alle identità digitali. Il progetto è finanziato dal programma europeo Horizon 2020 e si concluderà alla fine di quest'anno. Nello specifico, si propone di sviluppare una piattaforma conforme con i principi del GDPR per la protezione dei dati personali e che sia utile come attività di supporto e guida alla gestione e al trattamento dei dati stessi. Dopo l'identificazione sicura con eID per l'accesso alla piattaforma, l'utente è in grado di controllare, autorizzare e revocare l'uso delle PII che lo riguardano a specifici fornitori di servizi. Così facendo ci si trova di fronte a una situazione risolutiva di tipo win-win: da una parte gli utenti hanno a tutti gli effetti il controllo sui loro dati, dall'altra le organizzazioni vengono agevolate sul fronte della necessità di garantire la privacy degli utenti e la conformità alle norme [95].

Una volta effettuata l'autenticazione, la piattaforma PoSeID-on si presenta come una dashboard user-friendly (Privacy Enhanced Dashboard — PED) da cui si accede alle varie funzionalità. Viene realizzata sfruttando due tecnologie che assicurano lo scambio sicuro e una corretta gestione delle PII: queste sono blockchain e smart contract. All'interno di questa linea, il blockchain network controlla le autorizzazioni al trattamento dei dati e la gestione delle PII, ma non può salvare o trasmettere i dati in sé. Inoltre, consente di tenere traccia dell'attività svolta dagli utenti relativamente alle transazioni inerenti alle PII in ottica di accountability [95 e 96].

Le caratteristiche della blockchain la rendono una tecnologia ideale per la tutela della privacy degli utenti: è costituita da un network decentralizzato di componenti alla pari, in modo da eliminare gli svantaggi in termini di vulnerabilità dati da un'unica autorità centrale; si basa sul consenso diffuso dei partecipanti al network e permette di verificare in modo trasparente ed esteso le transazioni; infine le transazioni risultano molto difficili da modificare o manipolare perché vengono registrate su una sorta di "libro mastro" distribuito a un gruppo di partecipanti selezionati [97].

Allo stesso tempo, attraverso gli smart contract viene assicurata la privacy nelle transazioni perché si attua un procedimento per cui solo la persona a cui effettivamente spettano può ricevere i dati, garantendo così i principi di confidenzialità, inviolabilità e controllo degli accessi [95 e 96]. Per gestire il livello di rischio, il flusso di dati e lo sviluppo di avvertimenti di anomalie o transazioni sospette, vengono inseriti degli elementi architetturali: questi sono un modulo di gestione del rischio (Risk Management Module — RMM) che fa uso di algoritmi di machine learning per esaminare i diversi tipi di informazioni provenienti dalla piattaforma, e un analizzatore dei dati personali (Personal Data Analyzer — PDA) in grado di individuare i dati personali per cui non è stata data l'autorizzazione nelle transazioni. Tutte queste caratteristiche nell'insieme fanno in modo che l'utente possa gestire consapevolmente i propri dati e che sia in grado di disabilitare eventualmente i servizi che sono maggiormente soggetti a rischio [96 e 98].

L'utente che accede alla dashboard può evidenziare quattro elementi caratterizzanti. Il "portfolio wallet" contiene al suo interno le PII legate all'utente: attraverso questa interfaccia è possibile esaminare le PII e i servizi attivi. Si possono gestire le autorizzazioni di accesso, aggiornare e aggiungere PII in un'unica soluzione, con la consapevolezza che gli eventuali aggiornamenti verranno poi automaticamente recepiti dalle terze parti senza necessità di ulteriori azioni da parte dell'utente. Nella sezione "list of services" l'utente può visualizzare una lista di servizi disponibili presso terze parti, attivare nuovi servizi e monitorarne lo status. La terza componente, "log record", consiste nello storico comprensivo di data e ora di tutte le transazioni effettuate in merito ad esempio all'accesso dell'utente alla dashboard o all'utilizzo delle PII. Infine, il "risk management and data analyser" permette di visualizzare un punteggio del rischio di ciascuna PII associata a un determinato servizio e di monitorare le transazioni che non sono state ricevute o approvate dai destinatari interessati [99].

La piattaforma PoSeID-on è testata da una serie di progetti pilota inseriti in contesti pubblici, privati e misti in Italia, Francia, Spagna e Malta. Questi sono tutti accomunati da un iniziale bacino di utenti limitato e dalla sperimentazione in ambienti controllati e calati in contesti di vita quotidiana. Relativamente al pilot italiano, questo viene gestito dal Ministero dell'Economia e delle Finanze (MEF) nell'ambito della remunerazione dei dipendenti pubblici attraverso il portale NoiPA. Il portale è interessante ai fini del progetto in quanto gestisce un'incredibile quantità di consensi al trattamento di dati di carattere amministrativo ed economico appartenenti ai dipendenti pubblici italiani. Il progetto prevede l'integrazione di NoiPA con PoSeID-on. A quest'ultimo, attraverso SPID accederanno una cerchia selezionata di utenti che potranno dare il consenso a NoiPA al trattamento delle loro PII. Ai fini del test queste saranno solamente nome, cognome e indirizzo. I servizi resi disponibili saranno tre: si potrà modificare l'indirizzo di residenza e l'IBAN, oppure consentire a Reale Mutua Assicurazioni di avere accesso ai dati utili alla stima

dell'assicurazione di un veicolo in possesso dell'utente. Trattandosi di un test di carattere sperimentale, i dati utilizzati saranno falsi [98 e 99].

Il pilot francese invece è calato nel settore privato, in particolare in un'azienda privata che sviluppa software (Softeam). Il progetto si inserisce in e-Citiz, una piattaforma sviluppata da Softeam e già esistente che consente di monitorare e ottimizzare i processi aziendali tanto pubblici quanto privati. All'interno di e-Citiz è presente un servizio (SVE) per inoltrare qualsiasi tipo di richiesta a un'azienda. Ai fini del progetto pilota, SVE allora dovrebbe integrarsi con PoSeID-on in termini di creazione di un'unica piattaforma che controlli i dati personali. Infatti, SVE richiede all'utente l'inserimento dei propri dati personali per ogni singola richiesta inoltrata, e quindi appare ottimale per testare le soluzioni di PoSeID-on. In particolare verranno sperimentate le caratteristiche per gli utenti finali di un singolo servizio "Privaciz" in merito a sottoscrizione, condivisione dei dati, lista delle autorizzazioni e revoca della condivisione. I dati usati al fine del progetto saranno falsi [98 e 99].

Il caso studio spagnolo si svolge invece a Santander nell'ambito di digitalizzazione delle procedure amministrative, dove è stato raggiunto un importante traguardo consistente in più di 60 servizi resi disponibili on-line. La piattaforma locale che permette l'accesso ai servizi è eXperta ed è sviluppata da Munitecnia, un'azienda specializzata tra l'altro in amministrazione digitale. Il pilot allora si svilupperà come sperimentazione delle soluzioni PoSeID-on dal punto di vista dei cittadini utilizzatori dei servizi on-line e dell'amministrazione che tratta i dati forniti per l'espletamento dei servizi. L'utente quindi attraverso la piattaforma PoSeID-on potrà monitorare in un'unica soluzione un sottoinsieme delle PII di sua pertinenza per accedere ai servizi di eXperta. Chiaramente i servizi di eXperta da includere nel test saranno limitati a tre: la richiesta di rilascio o rinnovo di un permesso per parcheggiare all'interno delle linee blu, l'autorizzazione al possesso di animali ritenuti pericolosi, e infine un modulo di richiesta generale da compilare per ciò che non rientra in nessuna procedura standard. Come servizio aggiuntivo esterno invece è prevista la possibilità di inoltrare l'iscrizione all'associazione sportiva

municipale. L'obiettivo finale è quello di instaurare maggiore fiducia nei servizi on-line, di incrementare l'uso degli stessi e di consentire al Comune di rispettare le norme del GDPR [99].

Infine l'ultimo pilot si svolge a Malta, dove MITA (Malta Information Technology Agency) ha selezionato ai fini della sperimentazione un servizio di eGovernment gestito da Business First. Questo ente pubblico permette sostanzialmente di avviare un'impresa e ha il compito di raccogliere tutta una serie di informazioni che poi distribuisce autonomamente ad altri uffici pubblici di competenza. Le informazioni vengono raccolte attraverso una procedura on-line (eForm) che provvede a informare gli utenti della condivisione delle PII con terze parti. L'eForm è interessante nel contesto di integrazione con PoSeID-on perché attua una condivisione di informazioni con un numero consistente di destinatari. Inoltre, attualmente l'utente, dopo un iniziale consenso al trattamento dei dati, per apportare delle modifiche dovrebbe rivolgersi a ogni singolo ente a cui sono stati trasmessi i dati. Con PoSeID-on invece si ottiene con un unico accesso la gestione totale delle proprie PII. Anche in questo caso ai fini del test viene creato un contesto ideale e vengono utilizzati dati fittizi [99].

CAPITOLO VI

L'uso delle eID e degli eServices nelle Pubbliche Amministrazioni

La Commissione Europea ogni anno finanzia uno studio che misura gli sviluppi sull'uso degli strumenti ICT all'interno del settore pubblico per ciascun Paese europeo. L'eGovernment Benchmark viene calcolato sulla centralità dell'utente, sulla trasparenza, sull'uso di fattori chiave e sulla capacità di produrre servizi transfrontalieri in ottica di mercato unico europeo [105].

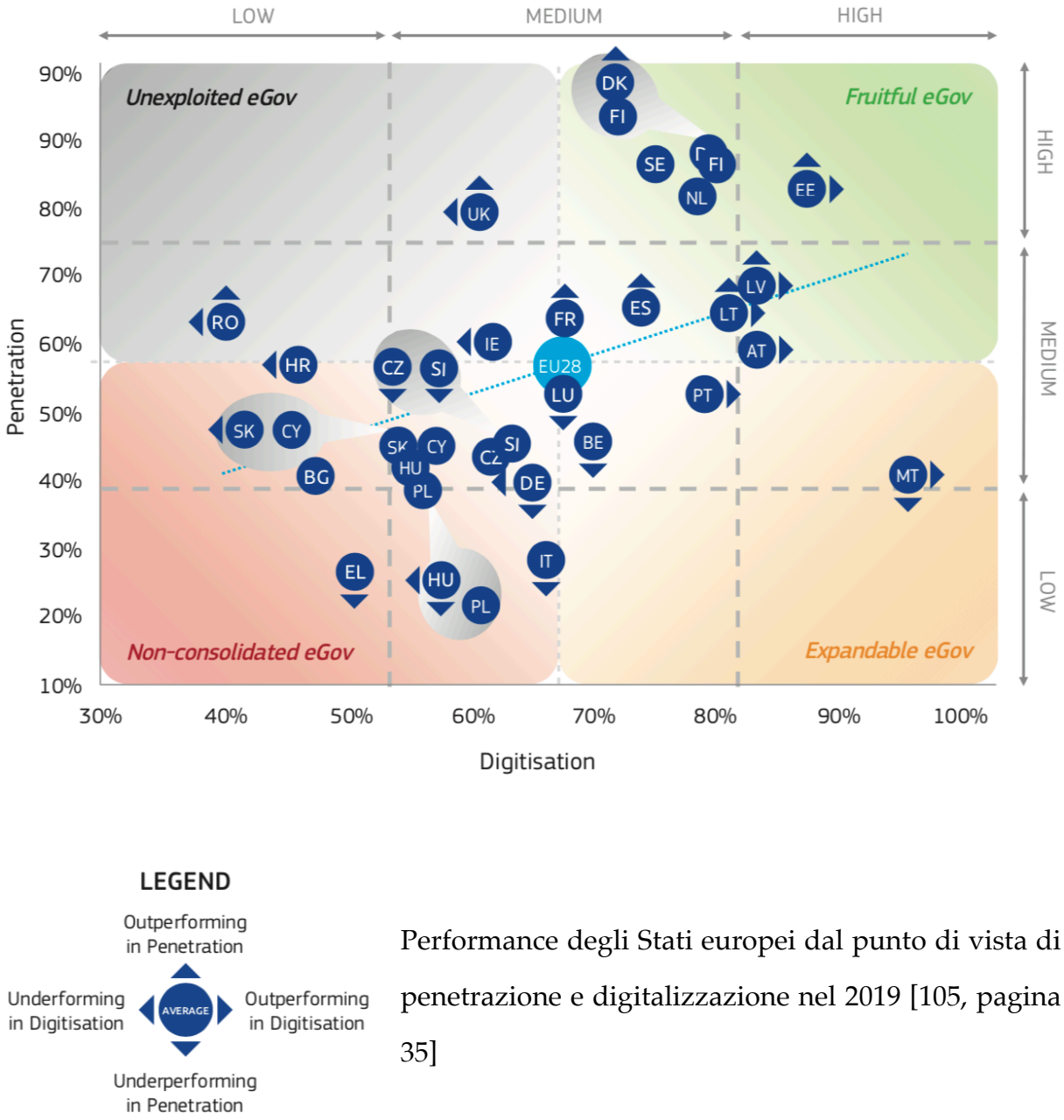
Se si guardano i risultati medi, la centralità dell'utente raggiunge il punteggio più alto tra gli indicatori con un 85%, il quale viene calcolato da fattori come disponibilità on-line, fruibilità e facilità d'uso da dispositivi mobili. La trasparenza raggiunge il 62%, mentre la mobilità transfrontaliera è tra i livelli più bassi con il 53%. Anche l'uso di fattori chiave come eID o altre forme di autenticazione digitale risulta ancora basso con un punteggio del 58% [105].

Tra i maggiori problemi evidenziati in generale vi è la disparità tra come vengono gestite le informazioni per le imprese e per i cittadini: infatti solitamente le procedure per usufruire di servizi pubblici on-line sono solitamente molto più chiare per i primi. Inoltre, la cybersicurezza non raggiunge ancora livelli ottimali. Gli altri elementi che necessitano di ulteriori miglioramenti sono l'incremento di servizi on-line e l'abbattimento delle barriere per gli utenti che accedono ai siti web istituzionali dai cellulari [105].

I due indicatori che riassumono tutto lo studio sono quelli che nel grafico a dispersione della pagina seguente sono posti sui due assi x e y. La "penetrazione" riassume in che misura vengono usati gli strumenti on-line a favore di servizi pubblici. Allo stesso tempo, la "digitalizzazione" misura quanto è stato digitalizzato all'interno degli uffici pubblici. Oltre a questo però è importante guardare anche ai fattori di correlazione. L'indicatore "penetrazione" è collegato alle abilità digitali, all'uso di tecnologie ICT e alla qualità dei servizi pubblici, mentre la

"digitalizzazione" è influenzata sempre dalle caratteristiche dei servizi ma anche dalla connettività. Oltre a questo, l'uso viene anche condizionato dalla percezione di fiducia verso le istituzioni di uno Stato e dalla sensazione che si ha della qualità dei servizi [105].

Parlando invece dei risultati tra i Paesi, emerge che i più performanti sono Malta, Estonia ed Austria, seguiti da Lettonia, Lituania e Finlandia. Al contrario, gli Stati del sud-est europeo hanno risultati ben al di sotto della media, con un divario di 42 punti tra il più performante e l'ultimo della classifica [105].



Performance degli Stati europei dal punto di vista di penetrazione e digitalizzazione nel 2019 [105, pagina 35]

La figura mostra il punteggio ottenuto da ciascun Paese secondo i due indicatori descritti precedentemente. Le frecce nelle quattro direzioni stanno ad indicare se un Paese ha performance di digitalizzazione e penetrazione che sono in linea con i risultati che ci si aspetterebbe in base ai fattori di correlazione [105].

Nelle pagine seguenti allora verranno prese in esame alcune delle best practices a livello europeo da cui sarebbe importante prendere spunto. Questo appare vero soprattutto alla luce delle soluzioni che vengono testate da anni con buoni risultati, e che per questo presentano maggiore affidabilità per eventuali implementazioni nella zona europea. In tutti i casi c'è correlazione tra l'essere smart city e offrire servizi pubblici digitali, dove più una città abbraccia i paradigmi dell'innovazione, più si dota di servizi digitali efficienti e numerosi per i suoi abitanti.

6.1 Il caso dell'Estonia: uno Stato all'avanguardia

L'Estonia è il Paese dei servizi pubblici digitali (eServices). Questa definizione rispecchia il grandissimo lavoro portato avanti dal Paese negli ultimi vent'anni verso la digitalizzazione. È anche una delle nazioni più connesse del mondo per la diffusione di internet e della partecipazione dei cittadini alla vita on-line. L'uso di internet viene visto infatti come un diritto dai cittadini, tanto che il 99% di loro nella fascia 16-74 anni ne fa uso, anche grazie a una copertura totale di rete per cellulari con tecnologia minima 4G (la 3G è in via residuale) e ai numerosi luoghi pubblici dove viene offerta la connessione Wi-Fi gratuita. Il traguardo raggiunto è davvero straordinario: per vederlo attraverso un dato, si può dire che in Estonia il 99% dei servizi pubblici è accessibile on-line tramite un unico portale (eesti.ee). Sostanzialmente vi è compreso tutto, eccetto matrimoni, divorzi e acquisti di immobili. Tutti i servizi disponibili sono accessibili tramite eID nell'ottica di parità tra autenticazione on-line e di persona, mentre le firme elettroniche sono legalmente

equivalenti a quelle autografe, sorpassando di gran lunga l'utilizzo di queste ultime. Non solo, perché l'Estonia è stata anche precursore del principio once-only, previsto nell'ordinamento interno già dal 1997 [106]. Sul fronte del risparmio ottenuto con i servizi digitali, stando ai report ufficiali, il Paese risparmia annualmente più di 1400 anni di lavoro e il 2% del prodotto interno lordo [107].

Secondo l'indice europeo DESI 2020, l'Estonia si posiziona settima. Il risultato è spiegato dal fatto che il Paese ha punteggi molto buoni negli indicatori di servizi pubblici digitali e capitale sociale, rispettivamente primo e terzo posto, mentre ha performance nella media nell'integrazione delle tecnologie nell'economia e nella connettività [108]. Da questo si capisce come l'Estonia abbia investito molto sulle infrastrutture per usufruire dei servizi digitali, ma manca forse di partecipazione o co-creazione da parte dei cittadini nel settore privato, dove rimane molto ampio il margine di espansione riguardo la digitalizzazione delle imprese [108 e 109].

Il mix vincente di attori che ha portato a "e-Estonia" è dato dalla sinergia tra Stato, settore ICT e una popolazione estremamente pronta ad accogliere i cambiamenti tecnologici proposti. Oltre a questo, si è puntato molto sull'introduzione diffusa della banda larga, su soluzioni che permettessero lo scambio sicuro di dati e sulle identità digitali. Gli investimenti in una società ICT sono da ritenersi una vera e propria scelta strategica da parte dello Stato, cosa che ha portato a un miglioramento della competitività e del benessere del Paese, e che ha ridotto drasticamente il fatto di rivolgersi fisicamente agli sportelli degli uffici pubblici, seguendo un principio di "riduzione dello Stato", anche se solo apparente [106]. A parte questo, si tratta anche di un fattore prettamente culturale: gli estoni si fidano del proprio governo e del settore pubblico in generale, e chi infrange le regole viene punito severamente [110]. Oltre a questo, lo sviluppo dell'ICT si può spiegare in parte anche come volontà di allontanarsi dal passato sovietico e di abbracciare quello che rappresentava il mondo occidentale [109].

Per capire però come funziona tutto questo apparato che supporta la digitalizzazione dell'Estonia, bisogna parlare di X-Road. Questo consiste in un

sistema virtuale sicuro pensato appositamente per lo scambio di dati in ambito di servizi elettronici, e per questo collega tra loro i vari database presenti sul territorio nazionale, assicurando una comunicazione protetta seguendo tra l'altro il principio dell'interoperabilità. La sicurezza viene garantita da dati criptati o autenticati mediante firme elettroniche. A usare X-Road sono più di 2300 tra servizi pubblici e privati. Lo Stato inoltre controlla il PKI (Public Key Infrastructure), un'infrastruttura che garantisce la sicurezza delle autenticazioni, della crittografia e delle firme [106].

Un altro punto importante che spiega la diffusione dei servizi digitali è la qualità del sistema di identità digitale dell'Estonia, che vanta la prerogativa di essere uno tra i più sviluppati del mondo. Tutto inizia dalle banche che con i loro servizi digitali sempre più diffusi iniziano ad emettere dei sistemi per autenticarsi in modo sicuro; oltretutto, si occupano anche di insegnare ai propri utenti come utilizzare gli strumenti tecnologici. Perciò il terreno era già preparato quando nel 2002 avviene la svolta con l'identità digitale pubblica: i cittadini del Paese possono (e devono se è scaduta la precedente) richiedere la carta d'identità elettronica (national ID-card), il cui chip contiene delle chiavi crittografiche dedicate. L'ID-card permette l'autenticazione sicura on-line oltre che la funzione di riconoscimento ai fini dell'identificazione fisica, ma anche la possibilità di firmare o criptare documenti. Può essere utilizzata eventualmente anche in sostituzione della patente, dato che gli agenti di polizia hanno i mezzi per effettuare controlli incrociati a partire dalle informazioni che ottengono dalla carta. Tutte queste funzioni sono accessibili utilizzando un card reader. Con l'emissione della carta viene anche associato a ciascun cittadino un indirizzo e-mail pubblico emesso dallo Stato: non si tratta di un vero e proprio indirizzo di posta, ma piuttosto di un intermediario che inoltra i messaggi all'e-mail usata dal cittadino. Tuttavia l'ID-card non è l'unica soluzione percorribile per accedere al mondo digitale: in Estonia infatti ci sono diverse tipologie di identità digitale a disposizione. Tra queste vi è ad esempio una "Mobile-ID" che offre sostanzialmente le stesse funzioni della carta nazionale (tranne la crittografia) ma con il supporto di un telefono, il quale integra la funzione del card reader. Per

accedere alle funzioni di Mobile-ID è necessario ricorrere a una SIM speciale adibita al servizio da sostituire ogni tre anni e contenente le chiavi private. Vi è poi Digi-ID, che si configura come un plus digitale dell'ID-card e come un documento in formato digitale fornito dallo Stato per l'identificazione elettronica e le firme. Tuttavia non può essere utilizzata per il riconoscimento fisico perché è stata pensata per un uso puramente on-line [106 e 111]. Infine l'ultima novità è Smart-ID, un'applicazione per cellulari che permette l'identificazione digitale e la creazione di firme elettroniche senza ricorrere al prerequisito della SIM card [112]. A oggi l'uso dell'eID è pienamente accettato dai cittadini, che ne fanno uso per due terzi su base regolare [113].

Non deve essere negato il fatto che il sistema presenta pur sempre delle fragilità: nel 2007 ad esempio è avvenuto uno degli episodi più gravi, dove i principali siti istituzionali sono stati colpiti da attacchi DDoS. Per paura di nuovi attacchi allora nel 2017 sono state trasferite delle copie dei dati sensibili provenienti da database nazionali verso una piattaforma cloud, la quale ha il suo database in una "ambasciata dei dati" con sede in Lussemburgo, ma sempre sotto la giurisdizione estone. A dispetto dei problemi che possono avvenire normalmente in qualsiasi contesto, tutti questi eventuali malfunzionamenti vengono visti sempre come opportunità di miglioramento a favore di una maggiore sicurezza, e con gli anni questo ha portato all'incredibile sviluppo di cui parliamo oggi [110].

Tra i servizi digitali che vale la pena menzionare, l'e-Banking è forse il meno recente perché inizia la sua strada nel 1996, ma rimane sicuramente uno tra i più consolidati ed efficienti del Paese. Le misure prese dalle banche per favorire la sicurezza e la fiducia dei cittadini nelle soluzioni on-line hanno fatto sì che si diffondesse in modo incrementale l'uso delle identità digitali. Oggi, l'unica occasione in cui è richiesto recarsi presso una filiale è l'apertura del conto, mentre per tutte le altre operazioni basta autenticarsi con eID. In vent'anni, si è arrivati alla quasi totalità delle transazioni effettuate on-line [106].

Più avanti, nel 2000 viene creato un sistema elettronico per la compilazione del calcolo delle tasse (e-Tax Board), mentre dal 2002 si può accedere direttamente alla dichiarazione precompilata con e-ID, apportare eventuali modifiche manualmente e infine firmare digitalmente. La caratteristica singolare del processo è che richiede dai tre ai cinque minuti, e per questo è usato dalla quasi totalità dei contribuenti. Inoltre, sempre sull'onda dell'efficienza, i rimborsi vengono effettuati in soli cinque giorni [106].

Vi è poi sempre dal 2000 un altro servizio pienamente abbracciato da tutte le strutture di parcheggio a pagamento, siano esse pubbliche o private. Si tratta di m-Parking, un sistema che permette di pagare il parcheggio direttamente dal proprio telefono attraverso un'apposita applicazione che rileva la localizzazione, oppure mandando un SMS. È poi l'autorità competente, dopo aver fatto delle verifiche, a mandare conferma della corretta registrazione del parcheggio. Quando si ha finito di usufruire del parcheggio si può aggiornare la propria situazione ricorrendo all'app, oppure è possibile mandare un secondo SMS. Alla fine del mese il costo dei parcheggi viene addebitato al credito telefonico. Il sistema funziona talmente bene che circa il 90% dei parcheggi viene pagato con questa modalità [106].

A Tallinn dal 2004 è sbarcato l'e-Ticket, una soluzione che coniuga al suo interno la possibilità di usufruire di biglietti personalizzati dei mezzi di trasporto pubblici (ma solo per i residenti e alcune categorie specifiche). Spariscono così i biglietti cartacei: i titoli di viaggio sono acquistabili online e vengono caricati sulla carta d'identità elettronica, utilizzabile per la validazione sui mezzi [106].

Sicuramente pionieristica risulta l'iniziativa di i-Voting avviata già dal 2005. L'internet voting è un sistema di voto addizionale che si affianca a quello classico, voluto appositamente per aumentare l'accessibilità al voto per le elezioni locali e nazionali. Infatti il cittadino può esprimere la sua preferenza da qualsiasi ubicazione (anche estera) senza doversi recare fisicamente ai seggi. Gli unici elementi indispensabili sono una connessione internet e l'identità digitale: quest'ultima permette l'autenticazione in uno speciale periodo di "pre-elezioni", dove i votanti

possono esprimere la loro preferenza ed eventualmente cambiarla (il voto precedente viene annullato), sfruttando un sistema che permette di non comunicare alla commissione elettorale l'associazione tra voto specifico e identità dell'elettore. Una volta che si chiude il periodo di "pre-elezioni", viene formata una lista dei cittadini che hanno già votato, così da impedire un potenziale doppio voto. Per dare un'idea dei dati, nelle elezioni parlamentari del 2015 hanno usato i-Voting circa il 31% degli aventi di diritto, molti dei quali hanno sfruttato questa opportunità per votare da ben 116 paesi [106]. Nel 2019 invece durante le elezioni del parlamento europeo, il 44% dei cittadini ha votato on-line [114].

Interessante appare anche il sistema di e-Business (anno 2007), una piattaforma on-line che si collega direttamente al registro di imprese e di persone legali dell'Estonia. Con l'autenticazione elettronica, gli imprenditori possono accedere a diversi servizi, tra cui la possibilità di avviare un'attività mediante una procedura interamente digitale della durata di 18 minuti. Tra gli altri vantaggi si trovano il poter visualizzare i dati e le tasse arretrate di un'impresa, diverse tipologie di report annuali ed eventuali relazioni tra imprese e persone [106].

Dal 2008 a oggi è stato implementato il sistema di e-Health: questo comprende sostanzialmente tutti i dati provenienti dai diversi fornitori di servizi del settore sanità, e ciò che ne consegue è la realizzazione di una cartella con la storia clinica per ciascun paziente a cui possono accedere tutti gli operatori sanitari abilitati. I pazienti, tramite identificazione elettronica, hanno la possibilità di visionare tutti i loro dati clinici, tra cui il medico di famiglia, visite effettuate, prescrizioni, e possono anche accedere a consulti medici. In casi di emergenza, i medici accedono ai dati essenziali di un paziente usando la carta d'identità. In generale, tutti i dati raccolti dal sistema di sanità digitale vengono elaborati in forma anonima per mettere a punto delle statistiche: ciò permette di allocare in modo efficace le risorse dello Stato e di realizzare studi sui trend di ambito sanitario. Dal 2010 all'interno di e-Health compare e-Prescription, uno tra i servizi digitali più apprezzati dai cittadini estoni. Le prescrizioni dei medicinali sono diventate digitali attraverso una procedura on-

line: il cittadino deve solo presentare la carta d'identità al farmacista che accede alle informazioni sul paziente e compila la prescrizione. Inoltre, per i rinnovi delle prescrizioni, non è necessario recarsi fisicamente dal medico, ma basta contattarlo tramite e-mail o telefono [106].

Uno degli elementi più discussi e innovativi è però e-Residency (anno 2014), un sistema transnazionale che permette di rilasciare identità elettroniche ai non residenti. Chi ne fa richiesta quindi riceve una smart card protetta da appositi certificati. Lo scopo del progetto è quello di consentire l'accesso sicuro ai servizi on-line dello Stato e la firma di documenti informatici. Uno tra i servizi a cui si può accedere è la registrazione di un'impresa e la gestione della stessa dall'estero, elemento interessante per eventuali investitori stranieri e allo stesso tempo soluzione unica per promuovere l'economia estone seguendo un'ottica a dir poco visionaria di potenziali "stati senza frontiere". Chiaramente questo non ha niente a che vedere con il conferimento della cittadinanza o con il permesso di entrare nel Paese senza visto, ma si configura piuttosto come una porta privilegiata per fare affari nel Paese e in Europa. A oggi vi sono più di 60 mila e-residenti contro i circa 10 milioni delle previsioni. Tuttavia i benefici che hanno dato luogo non sono da sottovalutare: si parla di 13 mila nuove imprese, per un totale di più di 30 milioni di euro di tasse solo nell'ultimo anno [106 e 115].

Tallinn, capitale e cuore dell'Estonia, è una smart city da cui si diffondono la maggior parte delle novità legate all'eGovernment. Per la notevole trasformazione digitale, Tallinn ha vinto il premio Netexplo Smart Cities 2020. I concetti alla base della filosofia della città sono infatti accessibilità, interoperabilità e l'essere user-friendly. La partecipazione e la co-creazione è ottenuta principalmente con sondaggi, ma non viene ancora sfruttata al massimo. Per coinvolgere più profondamente i cittadini, è stata lanciata ad esempio l'app AvaLinn, dove gli utenti possono condividere le proprie idee e opinioni sulla pianificazione degli spazi della città. A Tallinn i servizi digitali che richiedono autenticazione sfruttano l'eID nazionale: l'obiettivo è quello di fornire servizi interamente on-line che per ora sono 92, mentre

quelli parzialmente digitali sono più di 500. Oltre a e-Ticket, è possibile ad esempio richiedere il bonus bebè, supportare attività non-profit, richiedere licenze e permessi di qualsiasi tipo, allocare a uno specifico ente il bonus sport del comune, accedere a risorse degli archivi digitali, iscrivere i propri figli alla prima elementare, registrare una nascita e molto molto altro [116].

L'esperienza dell'Estonia e di Tallinn ha ispirato e continua a ispirare tutto il mondo per lo sviluppo senza precedenti delle soluzioni digitali, a partire dai Paesi nordici più vicini fino ad arrivare agli Emirati Arabi. Per il futuro il focus sarà l'uso delle intelligenze artificiali (AI) calate in specifiche soluzioni per il settore pubblico e privato. Secondo la strategia AI, i servizi saranno più semplici da usare, sarà più agevole analizzare i dati e verrà incrementato ulteriormente il livello di efficienza dei servizi pubblici. Oltre a questo, l'obiettivo è anche quello di attrarre investimenti stranieri interessati alle soluzioni di utilizzo delle AI [108].

6. 2 Il modello della Spagna e di Barcellona

La Spagna è uno dei Paesi più sviluppati se si parla di e-Government. Infatti all'interno dell'indice DESI 2020, all'indicatore servizi pubblici digitali si colloca seconda dopo l'Estonia. Ad esempio, viene premiata nel 2014 dalle Nazioni Unite per la creazione di una piattaforma da cui reperire i dati già in possesso delle amministrazioni secondo l'ormai noto OOP [125]. Tra gli elementi che possono spiegare in parte il motivo del successo del sistema di funzionamento dell'eGovernment si può includere la qualità dei servizi pubblici offerti, il profilo sociodemografico dei cittadini e il livello di soddisfazione nell'uso dei servizi [126].

Per accedere ai servizi digitali spagnoli e ricevere le informazioni utili basta collegarsi al portale principale conosciuto come "Punto de Acceso General" (administracion.gob.es) dove ciascun utente può visualizzare il proprio "raccoglitore del cittadino", il quale contiene tutte le informazioni e i procedimenti

che lo riguardano. Per accedere è necessario utilizzare l'autenticazione sicura della piattaforma "Cl@ve", il sistema unico per usufruire dei servizi della Pubblica Amministrazione e per le firme elettroniche. Cl@ve autentica il richiedente seguendo tre possibili vie: con un certificato digitale o carta d'identità elettronica (eDNI), con un PIN (quasi one-time), e con una codice semi-permanente. La piattaforma è pienamente interoperabile e assicura il riconoscimento transfrontaliero grazie al collegamento con il nodo eIDAS [127]. Un'altro elemento da sottolineare è che la carta d'identità elettronica da sola permette già di realizzare firme elettroniche di documenti e di provare in modo univoco la propria identità in rete. Analogamente alle carte europee quindi contiene all'interno del chip un certificato di autenticazione e un certificato di firma. Oltretutto, a differenza di CIE, è già stata emessa per la quasi totalità della popolazione spagnola [128].

Anche in Spagna è possibile avvalersi ormai da anni di diversi servizi in rete, tenendo in mente però che vi sono disparità tra regioni. Tramite eID in generale si può effettuare la richiesta di certificati e del casellario giudiziale, fare dichiarazioni alla polizia, chiedere il permesso per costruire, inoltrare domande di borse di studio, accedere alla cartella clinica, agli appuntamenti e alle prescrizioni, registrare l'apertura di una nuova impresa, fare la dichiarazione dei redditi e cambiare indirizzo [128 e 129].

Tra le città che più hanno saputo sfruttare i vantaggi della tecnologia a favore dei cittadini, vi è Barcellona. Il suo caso è interessante e di rilievo perché si differenzia dalle iniziative di digitalizzazione più comuni, dove è il governo centrale a dare i più grandi input di trasformazione. Barcellona invece si presenta come una città che va oltre questo schema, e riesce a portare avanti la digitalizzazione seguendo un disegno municipale a sé [130]. Nell'ultimo ventennio infatti la città ha avuto un ruolo decisamente rilevante nella sfera dell'innovazione della città a cui molti hanno guardato come esempio, anche grazie alla caratteristica di fornire codici open-source nella maggior parte delle soluzioni implementate. Usufruire dell'open-source significa condividere con terze parti un software che potenzialmente può essere

modificato e migliorato; così da una parte si ottiene un risparmio in denaro, mentre dall'altra si crea una rete di scambio di soluzioni tecnologiche tra amministrazioni [131].

Barcellona è conosciuta in tutto il mondo per essere una smart city, specialmente negli anni dopo il 2010 con le iniziative interne al programma "Smart City Barcelona". Dal 2015 invece, con il cambio del governo della città, viene pensato un piano digitale per il periodo 2017-2020 dal nome "Barcelona Ciutat Digital". Questo ha l'intento di restituire il possesso dei dati ai cittadini e di promuovere la sovranità delle soluzioni tecnologiche. Un altro elemento chiave del programma è anche l'idea che i servizi pubblici debbano essere forniti sfruttando i canali digitali sin dalla loro progettazione [132]. Il successo del "modello Barcellona" è stato riconosciuto da diversi premi: nel 2014 è la prima a ricevere dalla Commissione Europea il premio come capitale europea dell'innovazione (iCapital) per aver sfruttato le nuove tecnologie nell'intento di avvicinare i cittadini alla città [133].

Secondo alcuni invece più che di smart city o digital city, ha senso parlare di "experimental city". Questo perché vengono promosse la consapevolezza del ruolo fondamentale che hanno la coppia cittadini-dati nelle scelte politiche, idee di politiche economiche alternative, la partecipazione attiva dei cittadini alle proposte seguendo dinamiche bottom-up, la considerazione di un grande insieme di portatori di interessi e infine l'istituzione di living labs come i luoghi per eccellenza in cui calarsi nei processi di creazione, sperimentazione e apprendimento guidati dai principi di innovazione sociale e tecnologica. Da ciò si deduce che la trasformazione della città è per sua natura multidisciplinare, guidata dai dati e profondamente radicata a un particolare contesto creato dalle necessità dei cittadini [132].

Il frutto di questo risultato è stato sintomo di strategie eterogenee che si sono susseguite con le diverse amministrazioni, e più recentemente si sono integrate con i principi del GDPR. In particolare, i pilastri fondamentali e su cui si è insistito con maggiore interesse sono lo sfruttamento degli Open Data, la collaborazione tra enti di ricerca, università ed enti pubblici e privati, il risparmio delle risorse energetiche per

il perseguimento della sostenibilità ambientale, la digitalizzazione e l'innovazione sociale. In particolare, quest'ultima è vista di pari passo con l'inclusione sociale [133].

La linea scelta da Barcellona allora sembra vedere l'individuo non solo come semplice cittadino che prende le decisioni in modo passivo, ma piuttosto come un consumatore con il diritto di esprimere se concorda o meno con l'implementazione di un'idea, e con la capacità di partecipare alla costruzione dell'idea stessa. Secondo questa prospettiva, l'individuo-utilizzatore allora viene posto al centro, e gli vengono date le possibilità e gli strumenti per relazionarsi con i diversi portatori di interesse e per stimolare dei cambiamenti a favore del miglioramento del contesto urbano. D'altra parte, i dati si configurano come bene comune a disposizione di tutti, con la convinzione che questo possa portare benefici diffusi e migliori servizi pubblici [132]. Per questo è stato creato un portale accessibile a tutti, Open Data BCN, dove sono raccolti i dati pubblici provenienti dalla città e dai cittadini in quasi 500 diversi dataset [134].

Tra i progetti più importanti voluti dal Comune rientra "Data Commons Barcelona", un programma che studia un nuovo codice etico e un modello economico e legale per la società digitale della città, con lo scopo di restituire il valore dei dati ai cittadini [135]. Secondo questa visione, gli Open Data acquisiscono un ruolo fondamentale nella vita delle persone, e quindi non è solo importante restituire questa fonte di potere agli utenti, ma è essenziale anche capire come vengono prodotti e gestiti questi dati [136]. Nel 2016 invece viene lanciata la piattaforma "Decidim Barcelona" (noi decidiamo) per favorire la partecipazione democratica dal basso alle politiche pubbliche [132]. Nel periodo 2016-2019 arrivano più di 10 mila proposte, la maggior parte delle quali viene approvata [137]. Sulla stessa linea nel 2017 viene istituita una sorta di comunità di ricerca, "Metadecidim Barcelona", con il compito di elaborare e monitorare gli input provenienti da Decidim Barcelona [132]. Con l'obiettivo di proteggere i dati personali garantendo il controllo in capo agli utenti è stato creato un sistema (DECODE — DEcentralized Citizen Owned Data Ecosystems) che registra tutte le transazioni di dati e permette di decidere con chi

condividere le informazioni personali e di monitorare a chi sono stati inviati i dati. DECODE ad esempio ha permesso a Decidim di chiedere i dati agli utenti per l'identificazione e di raccogliere firme interne alle petizioni, cosa che prima non faceva per timore di abuso nei confronti della privacy dei cittadini [137].

Avendo in mente un'evoluzione tecnologica in continuo divenire, il Comune di Barcellona ha voluto dedicare già dal 1990 un intero settore interno allo sviluppo di progetti inerenti a strumenti ICT per gestire in modo efficiente le risorse della città e migliorare la qualità della vita dei cittadini. Questo apparato è l'Institut Municipal d'Informática (IMI), e ad oggi si qualifica come importante punto di riferimento per guidare e dare supporto alle politiche sull'uso delle ICT [138].

A proposito di living labs invece, viene riqualificato un intero quartiere della città in cui stabilire un distretto (22@) per la promozione dell'innovazione sfruttando progetti pilota e sperimentazioni di strumenti tecnologici: al progetto partecipano portatori di interesse diversi come università, start-up e centri di ricerca [139].

La città conta anche di un'intera rete di sensori intelligenti, il cui insieme viene gestito da una piattaforma chiamata "Sentilo" [137]. I sensori sparsi per Barcellona sono migliaia (circa 20 mila), e ogni giorno raccolgono una mole incredibile di dati: il passaggio delle macchine, l'uso dell'energia, la raccolta dei rifiuti, il movimento delle persone, la qualità dell'aria e la presenza di diversi fattori atmosferici. Avere tutto questo materiale a disposizione permette di gestire al meglio la macchina che regola la città, come ad esempio la capacità di accendere i lampioni stradali solo quando fa buio [137].

A Barcellona, se guardiamo a come il cittadino può relazionarsi con la Pubblica Amministrazione, viene privilegiata la forma elettronica dall'origine, nel senso che eventuali nuovi servizi devono essere implementati in forma digitale. Inoltre, si specifica che rendere digitali tutti i servizi esistenti richiede un processo di trasformazione interna dell'amministrazione della città lontano da un procedimento meramente meccanico. Tuttavia, questo consente di accedere praticamente a qualsiasi procedura direttamente on-line, assicurando efficienza, efficacia e risparmio nel

compimento dei servizi. A questo proposito, il Comune ha una vera e propria sede elettronica: si tratta di uno spazio virtuale dove i cittadini possono trovare informazioni [140], e al cui interno, in ottica di semplificazione, viene pensato un unico punto di accesso elettronico a tutte le procedure amministrative, l'Officina Virtual [141]. I servizi disponibili da questo portale, il cui accesso è garantito secondo meccanismi di autenticazione che variano in base alla tipologia di servizio pubblico scelto, sono più di 200. Si tratta di un numero di servizi piuttosto importante, che permette ad esempio di presentare ricorso a una multa stradale o a un tributo pubblico, registrare una nascita, ampliare l'orario di apertura di un pubblico esercizio, chiedere il permesso per trasporti eccezionali attraverso la città o per la destinazione d'uso di zone carico-scarico merci, registrare la rottura di una coppia convivente stabile, chiedere il permesso per fornire servizi funerari, aggiornare il proprio indirizzo fiscale e l'indirizzo di residenza, e modificare il titolare d'imposta di beni immobili. Questi sono solo alcuni, perché bisogna dire che spaziano davvero in ogni ambito che coinvolge la vita nella città [142].

Riguardo i metodi di autenticazione on-line di persone fisiche, il Comune ammette principalmente la carta d'identità elettronica (eDNI); in alternativa è possibile l'autenticazione con firme elettroniche provviste di certificato digitale idCat emesso dalla regione della Catalogna (Consorcio de Administración Abierta de Cataluña), oppure di certificato digitale emesso dalla Fábrica Nacional de Moneda y Timbre. Per un gruppo più ristretto di servizi invece è possibile autenticarsi con Cl@ave o con idCat per cellulari [143]. Un ulteriore fonte di autenticazione per alcuni servizi pubblici cittadini è nata nel 2015: Mobile ID è attualmente riconosciuta da soli due comuni, tra cui per l'appunto quello di Barcellona. Attraverso l'app per cellulari, una volta che si sono completati gli step per la creazione dell'identità, è possibile autenticarsi per usufruire di servizi on-line, oppure firmare documenti elettronici [144].

L'evoluzione intrapresa da Barcellona è sicuramente tra le più virtuose e inclusive nel contesto mondiale e un ottimo esempio di dinamiche bottom-up nel

contesto di sviluppo urbano. Anche se il cammino è ancora lungo, i progetti implementati hanno avuto sicuramente un impatto positivo, semplificando la vita quotidiana dei cittadini e rendendo l'amministrazione della città più efficiente.

6.3 Milano: un esempio virtuoso nel contesto italiano

Milano è considerata la città più smart d'Italia per diversi aspetti (ICity Rate), a partire dalla solidità economica e dalla mobilità sostenibile, ma anche per gli ambiti di qualità sociale e trasformazione digitale, dove vengono valutati alcuni sotto-indicatori, come l'accesso alla banda larga, la disponibilità di servizi on-line, l'IoT e la creazione di app municipali. In questo contesto si è visto come le tecnologie hanno permesso di creare nuove opportunità nell'offerta di servizi urbani [153]. Il progetto che si propone di inserire Milano nel gruppo di città smart inizia nel 2012 e da quel momento sono stati fatti notevoli passi avanti verso il raggiungimento dell'obiettivo di indirizzo politico e strategico. L'idea che ha sempre guidato però questa linea è la chiara intenzione di non volersi limitare alla "città intelligente", la quale si avvale principalmente delle tecnologie per la sua evoluzione. Piuttosto, si vuole amalgamare altre tipologie di componenti all'interno di questo percorso di rinnovamento: parliamo soprattutto di inclusione sociale, partecipazione di un grande numero di attori, sviluppo economico, formazione e ricerca [154].

Le linee guida di Milano Smart City arrivano per la prima volta nel 2014. Nel documento emerge la consapevolezza che per creare innovazione è necessario ripensare le politiche della città. La Pubblica Amministrazione ha quindi il ruolo importantissimo di dare vita a quel contesto favorevole che possa fungere da volano alla trasformazione della città attraverso il contributo sinergico dei diversi attori [155].

I pilastri su cui si basa Milano Smart sono innanzitutto il voler essere città internazionale e modello per l'inclusività delle politiche urbane sostenibili. Poi

ancora si trovano la mobilità interna a ridotto impatto ecologico, una migliore gestione delle risorse energetiche, e l'inclusione delle varie parti sociali in ottica di rete, tenendo in considerazione tutti i gruppi a rischio di esclusione. Oltre a questo si punta sulla semplificazione dei processi amministrativi e sul fatto di permettere a tutti di reperire le informazioni di cui hanno bisogno nel modo più agevole possibile [155]. La cosiddetta trasformazione digitale si divide quindi tra i due paradigmi di tecnologia e cultura digitale, con particolare interesse a infrastrutture scalabili, servizi digitali di facile accesso e user-friendly, educazione digitale e digital skills per gli utenti e infine un approccio di fornitura dei servizi data driven [156].

Il lavoro fatto sull'infrastruttura innanzitutto comprende il piano di interoperabilità verso la connessione di tutti i servizi pubblici e una più agevole circolazione dei dati. Un altro punto importante da menzionare è il progetto "data lake", una sorta di archivio unico in cui far convergere i dati provenienti dal Comune di Milano secondo l'idea di connessione tra dati che prima erano sparsi nei diversi dipartimenti, così da sfruttare i benefici della correlazione e del machine learning per produrre politiche data driven. Oltre a questo, è stata favorita la scelta di adozione del 5G in tutta l'area metropolitana di Milano, abbinata all'offerta di una rete wi-fi pubblica, e la creazione di una dashboard a scopo di monitoraggio dei servizi forniti dal Comune da cui poter individuare agilmente problemi e feedback sui dati [157].

Guardando ai progetti sui servizi, l'elemento più interessante è forse il fascicolo del cittadino. Si tratta di una piattaforma che rappresenta un unico punto di accesso ai servizi digitali e che comprende al suo interno i documenti dei cittadini. Di recente è stata resa disponibile anche come applicazione per cellulari: si ha quindi un'interazione diretta e veloce tra Comune e cittadino, dove ad esempio per comunicare le scadenze vengono sfruttate le notifiche push. Dal fascicolo del cittadino si può chiedere certificati, informazioni sul nucleo familiare e documenti, pagare le tasse e le multe, effettuare iscrizioni agli asili nido, prenotare appuntamenti e scrivere al Comune. L'accesso viene stabilito mediante il canale sicuro di autenticazione SPID. In aggiunta al fascicolo, viene anche ripensato il sito web del

Comune, ponendo al centro dell'attenzione dell'utilizzatore la possibilità di usufruire dei servizi digitali [157]. Ad esempio, verificando la propria identità con SPID, è possibile richiedere tutta una serie di certificati, tra cui quelli anagrafici, senza dover visitare gli sportelli comunali. L'idea si sposa a favore dello stabilimento dei cosiddetti "Punti cittadino digitale", degli sportelli amministrativi fisici di accesso unico da cui l'utente dovrebbe poter far uso dei servizi on-line. Sempre facendo riferimento alla trasformazione digitale, si dà l'ulteriore possibilità di farsi recapitare estratti ed atti di nascita, matrimonio e morte mediante un indirizzo e-mail [158]. Parlando di numeri, negli ultimi mesi la percentuale di certificati che è possibile scaricare on-line è intorno all'80% [159], mentre i servizi on-line accessibili dal sito del Comune con autenticazione SPID sono attualmente circa un centinaio [160]. Infine, sul fronte dei pagamenti, dal 2017 a oggi Milano è riuscita a far raggiungere a pagoPA il traguardo di principale fonte di riscossione dei pagamenti comunali [157].

Per quanto concerne lo sviluppo delle competenze, Milano promuove una settimana (Milano Digital week) che ha come focus il tema del digitale visto come strumento di inclusività e innovazione, dove ad esempio vengono proposti corsi di formazione per accedere ai servizi digitali del Comune a favore degli over 60. Dal 2020 invece è presente un'iniziativa in collaborazione con l'ONU: è conosciuta come STEMinthecity (Science, Technology, Engineering and Mathematics) e si qualifica come piattaforma rivolta a utenti come studenti, insegnati e genitori. Lo scopo è quello di trasmettere in modo diffuso i principi della scienza e della tecnologia, e di restringere il divario di genere nell'avvicinamento allo studio di carattere scientifico tra ragazzi e ragazze [157].

Rispetto alle dinamiche imposte dalla pandemia del 2020, il Comune di Milano ha reagito con "Digital Care", un nuovo modo di vedere l'innovazione sostenibile e di prendersi cura dei cittadini durante l'emergenza. Secondo questo piano, l'elemento che ha costretto le persone a stare a casa è anche quello che ha sottolineato quanto il canale digitale sia fondamentale per consolidare l'inclusione sociale, e che ha dato una spinta ancora maggiore alla trasformazione digitale

sostenibile e scalabile [156]. In particolare, oltre alle pratiche piuttosto diffuse di smartworking dei dipendenti pubblici, è stata ampliata l'offerta di servizi digitali e si è cercato di semplificare gli stessi, sono state promosse iniziative per diffondere i servizi on-line anche con sportelli decentrati sparsi per Milano, ed è stato messo a disposizione un assistete virtuale (chatbot) in grado di interagire con l'utente che necessità di informazioni in merito alle nuove dinamiche in atto [161].

Milano si è esposta anche sul fronte della diffusione dei diritti digitali in partnership con altre città dal mondo unendosi a Cities Coalition for Digital Rights. Il gruppo, tra cui per altro Barcellona è una delle città fondatrici, sposa le idee dell'accesso a internet per tutti, dell'alfabetizzazione digitale, della protezione dei dati, della trasparenza, della democrazia partecipativa e di standard di servizio aperti e digitali [157].

Di seguito si propone una tabella riassuntiva delle principali caratteristiche messe a confronto [142,160,162].

caratteristiche/servizi	Estonia - Tallinn	Spagna - Barcellona	Milano
banda larga	✔	✔	✔
wi-fi pubblico	✔	✔	✔
database estero	✔		
open data	✔	✔	✔
servizi pubblici digitali	✔	✔	✔
partecipazione e co-creazione	✔	✔	✔
identità digitale per accesso ai servizi	✔	✔	✔
diversi tipi di identità	✔	✔	
mobile-ID	✔	✔	
smart-ID (app)	✔	✔	

caratteristiche/servizi	Estonia - Tallinn	Spagna - Barcellona	Milano
interoperabilità	✔	✔	
portale di accesso unico ai servizi	✔	✔	✔
i-Voting	✔		
e-Residency	✔		
certificati		✔	✔
registrazione nascita	✔	✔	
iscrizione a scuola	✔		✔
permesso di costruire		✔	✔
accesso cartella clinica	✔	✔	✔
registrazione nuova impresa	✔	✔	✔
dichiarazione dei redditi o pagamento tributi	✔	✔	✔
cambio indirizzo	✔	✔	✔
permesso abbattimento e potatura alberi	✔		
bonus bebè	✔	✔	✔
permesso per evento pubblico	✔		✔
permesso di parcheggio per residenti	✔	✔	✔
registrazione del proprio animale domestico	✔		

CAPITOLO VII

Elementi di criticità, barriere e considerazioni

A distanza di anni dall'apparizione in Europa delle prime eID di inizio secolo, il sistema non è stato pienamente perfezionato. Ci sono ancora dei problemi sull'implementazione e la diffusione delle identità digitali: è molto presente infatti la frammentazione, mancano standard e maggiore interoperabilità, e infine serve uno sviluppo della sicurezza per prevenire attacchi che negli anni hanno subito un incremento di frequenza sempre maggiore. In questa sezione allora vengono raggruppati diversi elementi in merito a problemi emersi durante la stesura dell'elaborato, nonché considerazioni e riflessioni finali.

7.1 Molteplicità identità digitali e correlazione servizi digitali - eID

La diffusione delle identità digitali è legata al numero di servizi in rete a cui gli utenti possono accedere. Infatti i cittadini possono mancare di motivazione se non vedono un ritorno dal possesso di identità digitale. D'altra parte però è anche vero il contrario: se il bacino di utenti titolari di identità digitali rimane marginale, non ci sarà interesse a incrementare gli eServices, perché naturalmente nessuno vuole investire se poi non ci saranno utilizzatori interessati a usufruire dei nuovi servizi. Questo è un problema dove una delle due parti deve necessariamente prendere una posizione: in questo il potere rimane nelle mani dello Stato, che diffondendo i servizi digitali, potrà dare uno stimolo alla richiesta di eID. È anche vero però che negli ultimi anni, ma soprattutto nel corso del 2020, c'è stato un incremento notevole, tanto di eID quanto di eServices.

Per alcuni invece la diffusione di troppe tipologie diverse di identità digitali può costituire una criticità perché fonte di confusione per gli utenti, e quindi può

rivelarsi addirittura controproducente al fine di riuscire ad associare ad ogni cittadino una corrispondente identità in rete. La considerazione fatta non è sbagliata, perché se lo scopo dietro l'idea di fondo dell'eID è semplificare e permettere l'accesso ai servizi con un'unica identità digitale, allora non si spiega come mai già ora vengano offerte diverse modalità per acquisire un'identità digitale invece di pensare ad accorpare questi sistemi (vedi ad esempio CIE e SPID). D'altra parte però è anche vero il contrario: può sembrare un controsenso, ma si può sostenere il fatto che offrendo più di un sistema di autenticazione, si può raggiungere un maggior numero di utenti. Poniamo per assurdo che SPID non esista, allora l'unica possibilità di avere un'identità digitale sarebbe attraverso CIE. Quest'ultima però si può richiedere a ridosso della scadenza della vecchia carta con massimo 180 giorni di anticipo. È palese che con questo metodo verrebbero esclusi un numero troppo elevato di utenti e per un periodo di tempo che non permetterebbe il conseguimento dell'obiettivo iniziale. Questa tesi è per altro sposata dai numerosi casi dove la diffusione di più tipologie di identità digitali costituisce la norma.

7.2 Servizi transfrontalieri e lingue di comunicazione

Se da una parte è vero che con eIDAS c'è l'obbligo di riconoscimento reciproco tra Stati membri in merito alle diverse identità digitali nazionali, dall'altra è tuttavia un elemento che in alcuni casi non è stato ancora recepito da tutti. A causa di questi ritardi quindi, il progetto del mercato unico digitale transfrontaliero non è stato pienamente realizzato.

Tra l'altro, a volte è presente un altro motivo di difficoltà. Anche la lingua di comunicazione è una barriera non indifferente. Capita ad esempio che i siti web siano ben tradotti almeno in inglese e presentino servizi digitali funzionanti. Tuttavia, nel momento in cui si vuole usufruire di uno specifico servizio attraverso il link "accedi con eIDAS", la pagina seguente non appare tradotta. Questo, come ci si

può aspettare, mette in difficoltà l'utente oltre confine e gli impedisce di proseguire. A questo proposito allora è necessario avere più cura nella traduzione di tutte le pagine web legate a istituzioni o servizi digitali. Non ha infatti senso che ci sia un impegno immenso nel far riconoscere un'identità digitale nazionale negli altri Paesi europei e rendere disponibili i servizi in senso transfrontaliero, se poi il processo viene bloccato da un impedimento di tipo linguistico che nell'insieme è sicuramente molto più semplice da aggirare.

7.3 Ulteriori fattori di esclusione: età e difficile comprensione

Nel momento in cui si implementano soluzioni pubbliche che hanno come prerequisito una conoscenza quantomai minima di informatica, bisogna tenere in considerazione che non tutti gli utilizzatori potrebbero avere questo bagaglio di nozioni. Inoltre, non tutti hanno accesso agli stessi strumenti, oppure non sono in grado di rapportarsi con il mondo digitale, e ciò pesa in modo incrementale con l'aumento dell'età.

Questo in parte può essere spiegato anche in termini di dati: la percentuale di popolazione europea con abilità digitali non ha subito grandi cambiamenti dal 2016, anzi, più del 40% non è capace di usare i servizi digitali. C'è quindi il rischio che anche incrementando e migliorando i servizi di eGovernment, mancherà all'appello una grande fetta di utenti perché senza gli strumenti adatti alla comprensione dell'evoluzione digitale, senza considerare il fatto che questo può causare per alcuni l'esclusione da servizi che teoricamente sarebbero pensati per essere universali. Il ristagno, almeno iniziale quindi, è uno scenario che non va escluso [105].

In aggiunta, bisogna anche tenere in considerazione che i servizi e le modalità di utilizzo delle identità digitali dovrebbero essere il più possibile elaborati per essere user-friendly. Infatti, complicare in modo eccessivo, anche banalmente rendendo troppi i codici da ricordare in merito alle identità digitali, potrebbe risultare

controproducente e allontanare ancora di più il cittadino dall'accesso alle piattaforme digitali.

7.4 Percezione, fattori socio-culturali e coinvolgimento del settore privato

È molto importante anche la percezione che hanno i cittadini verso le soluzioni digitali. Gli Stati dovrebbero favorire la consapevolezza dei cittadini della disponibilità di servizi digitali e di tutti i benefici che questi comportano. Oltretutto, pensando prevalentemente a fattori di carattere culturale, è necessario promuovere un senso di sicurezza e fiducia nelle identità digitali, dimostrando concretamente in che modo vengono gestiti i dati e quantificando il livello di pericolo per la privacy dei cittadini. Se al contrario prevale il senso di paura verso ciò che non si conosce o la sfiducia verso il governo del proprio Paese, il decollo di questi strumenti allora sarà più lento e faticoso.

Limitatamente alle dinamiche interne alle Pubbliche Amministrazioni, possono essere individuati ulteriori fattori che fungono da barriera a una diffusione più ampia delle identità digitali. Innanzitutto in alcuni casi può avere luogo una resistenza al cambiamento, che di conseguenza porta a un rallentamento generale e a uno sforzo maggiore verso il raggiungimento dell'obiettivo. Oltre a queste forze interne che rifiutano l'innovazione, bisogna anche considerare che una grande fetta dei dipendenti pubblici non ha le competenze adeguate per interfacciarsi con supporti di tipo informatico e gestire la fornitura dei servizi secondo le nuove modalità previste. Inoltre, in alcuni casi manca la collaborazione tra amministrazioni, che al contrario potrebbero supportare maggiormente attività di scambio e co-creazione nell'intento di mettere a disposizione soluzioni comuni e diffuse per combattere la frammentazione generale nell'offerta di servizi.

Le potenzialità che assicurano le identità digitali non sono circoscritte al settore pubblico ma si prestano molto bene all'uso nel settore privato, permettendo di

sorpassare l'onere derivante dalla gestione dei dati. Il settore privato però deve essere disposto a cogliere la sfida, e quindi fornire servizi che accettino l'autenticazione con eID. Tuttavia, le imprese private aderenti sono ancora molto poche, e i risultati di una loro partecipazione più importante si vedranno solo nei prossimi anni.

7.5 eGovernment e blockchain

Come si è già visto in precedenza, il sistema blockchain è una tecnologia relativamente recente, che permette di scambiare dati all'interno di un gruppo di utenti decentralizzato e formato da nodi (il cosiddetto scambio peer-to-peer). Più nello specifico i nodi costituiscono nel loro insieme un database in grado di registrare le transazioni in modo cronologico e permanente con una modalità di salvataggio dei dati associabile a una sequenza di blocchi, senza il coordinamento di un elemento architetturale centralizzato o di intermediari. I blocchi di dati aggiunti vengono uniti al blocco di dati immediatamente precedente con un sistema di crittografia e formano così una catena. Il network che sfrutta la blockchain presenta un meccanismo di consenso per cui tutti i nodi condividono la stessa identica copia di dati [171 e 172].

La tecnologia blockchain può portare sicuramente benefici per l'avanzamento dell'eGovernment, come ad esempio l'aumento dei servizi offerti, la semplificazione dei processi burocratici, la trasparenza e immodificabilità delle informazioni, l'affidabilità e la sicurezza dei dati, e infine la riduzione dei costi [171]. Concretamente, si può impiegare nell'approccio delle Self-Sovereign Identities (SSI), un sistema che non prevede una componente di gestione centralizzata delle identità. L'idea delle SSI si origina infatti con lo scopo di dare più spazio alla gestione dei dati da parte degli utenti e di migliorare la privacy degli stessi. Secondo questo sistema i dati comunicati a terzi sono solo quelli strettamente rilevanti. Ad esempio, se per usufruire di un servizio bisogna essere maggiorenni, allora l'identity provider darà

comunicazione positiva o negativa rispetto alla domanda in merito alla maggiore età, ma non specificherà la data di nascita dell'utente [173].

Le sfide sull'uso della blockchain in ambito di eGovernment allora riguardano la scalabilità del modello, la possibile fuga di dati, distorsioni delle transazioni dovute all'acquisizione illegale dei nodi da parte di utenti terzi, il pericolo di invalidità di alcune informazioni in determinati Stati e infine un possibile conflitto con il GDPR in merito a ciò che riguarda i dati personali. Secondo quest'ultima considerazione infatti c'è uno scontro: se da una parte il regolamento europeo ammette il diritto all'oblio, una delle caratteristiche fondamentali della tecnologia blockchain è proprio l'immutabilità dei dati. Inoltre, in base all'ampia definizione di dato personale del GDPR che comprende sostanzialmente qualsiasi elemento riconducibile alla persona, c'è il pericolo che, per la natura stessa della blockchain in quanto a pubblicità dei dati, l'identità dell'individuo non venga protetta [171].

Un altro possibile problema evidenziato è costituito dal controllo del 51% dei nodi: sostanzialmente, piuttosto che attaccare i sistemi crittografici, l'hacker opta per la strada più semplice e prende possesso della metà dei nodi più uno. Questo tipo di attacco gli permette di registrare dati non validi nel network. La vulnerabilità appena descritta è però tanto meno possibile da realizzare, quanto più è grande il gruppo di nodi che forma la blockchain [173].

7.6 Dubbi sui metodi di riconoscimento

In molti casi gli identity provider offrono ai richiedenti eID un servizio di riconoscimento da remoto. Questo però ha sollevato alcuni dubbi sulla sicurezza: il fatto di presentare una foto dell'utente e una foto del documento non tiene in considerazione una possibile manipolazione delle immagini, e lo stesso si dice per i video. In base quindi al pericolo che documenti, video e immagini vengano alterati, non c'è consenso sul fatto che il metodo di riconoscimento con web-cam possa

abilitare un livello di sicurezza elevato in base ai forti requisiti di sicurezza richiesti [173].

Sono emersi dei problemi anche sul fronte di verifica dei documenti a fronte di una richiesta di emissione di identità elettronica, specialmente quando si parla di strumenti di riconoscimento extra-nazionali. Se i responsabili della verifica dei documenti hanno una buona conoscenza dei documenti interni al loro Paese, si evidenzia il fatto che mancano di preparazione sui documenti stranieri, e per questo l'identificazione a tratti può risultare difficoltosa [173].

7.7 Complicazioni nell'autenticazione e sicurezza

I metodi di autenticazione inerenti ai cellulari, quali riconoscimento facciale e impronte, presentano a loro volta dei pericoli. Ogni dispositivo infatti ha dei suoi standard di sicurezza e sensori con diversi livelli di rischio di accettazione di false credenziali biometriche. Inoltre, spesso accade che a uno stesso dispositivo, vengano associati più profili di autenticazione, e questo ha conseguenze negative nel momento in cui viene fatto uso delle eID, perché bisogna capire chi tra gli utenti con accesso al cellulare è legittimato a usare effettivamente l'identità digitale in quanto titolare della stessa. Per questo motivo, è sconsigliato l'uso di queste forme di autenticazione biometrica per l'accesso alla propria eID, specialmente nei casi che impiegano il livello di sicurezza elevato [173].

Anche le One Time Password (OTP) tramite SMS ed e-mail non possono essere ritenute del tutto sicure, pur essendo soggette ad attacchi piuttosto difficili tecnicamente. Tuttavia, tra le due, la OTP tramite e-mail è altamente sconsigliata, perché è più facile per un hacker riuscire ad accedere illegalmente alla casella di posta dell'utente [173].

Infine, si possono evidenziare mancanze anche in merito alle componenti di sicurezza per l'uso delle eID, come ad esempio i chip. Queste infatti vengono

certificate per prevenire potenziali attacchi, ma ciò non è sufficiente. Sarebbe necessario pensare a una certificazione continua delle componenti, dato che, siccome le minacce di attacchi evolvono con rapidità, un certificato datato potrebbe non essere in grado di fornire la sicurezza adeguata. È opportuno preferire quindi metodi di certificazione continua [173].

7.8 Incidenti di sicurezza 2019 (report ENISA 2020)

I rapporti sugli incidenti in merito alla sicurezza denunciati dai fornitori di servizi fiduciari (Trust Service Provider — TSP) alla Commissione europea e a ENISA nel 2019 sono stati 32. Rispetto all'anno procedente, c'è stato un aumento considerevole di incidenti (80%), ma ciò non significa necessariamente un peggioramento generale delle condizioni di sicurezza. Infatti, ENISA afferma che questo dato è dovuto alla maggiore familiarità dei TSP con le procedure di denuncia delle falle dei sistemi [174].

Oltre a questo, si evidenzia come gli errori di sistema (hardware e software) siano la causa principale dei rapporti pervenuti. Le altre motivazioni sono invece errori di carattere umano e in piccola parte attacchi informatici (9%). Un altro dato interessante è che gli incidenti riguardano per più di tre quarti fornitori di servizi fiduciari qualificati (Qualified Trust Service Provider — QTSP), mentre i TSP non qualificati mostrano una ridotta quota di incidenti. Qui però va fatta una precisazione: il più delle volte le segnalazioni vengono fatte da TSP che offrono anche servizi qualificati, dove gli incidenti di sicurezza quindi riguardano tanto i servizi qualificati quanto i servizi non qualificati. Il dato allora mostra come venga sottostimato il numero effettivo di incidenti in merito ai servizi non qualificati. Oltre a questo, va anche evidenziato il fatto che il controllo sui servizi non qualificati avviene solo ex-post: gli organismi di vigilanza (Supervisory Bodies — SB) infatti hanno il potere di azione solo dopo che si è verificata una violazione della sicurezza.

Da qui deriva la difficoltà di intervento che spesso interessa i SB, perché questi ultimi spesso non vengono informati direttamente sugli incidenti e non hanno contatti diretti con i TSP non qualificati [174 e 2, articolo 17].

Riguardo invece l'entità dell'impatto data dagli incidenti, un terzo ha avuto effetti sfavorevoli consistenti, mentre aumenta il numero di incidenti minori, cosa che fa pensare a una migliore accuratezza e una maggiore familiarità con i meccanismi di denuncia [174].

Conclusioni

Nel corso dell'elaborato si è cercato di percorrere, a partire da differenti aspetti di studio, i principali elementi caratterizzanti della digitalizzazione della Pubblica Amministrazione in Europa. In particolare, l'attenzione è stata posta sulle identità digitali e sui servizi pubblici in rete a cui le prime consentono di accedere. Questo sembra ancora più interessante alla luce degli scenari aperti nel corso di quest'anno a causa della pandemia, che in molti casi ha portato a una notevole accelerazione di processi già in atto. Basti pensare alla velocità dei cambiamenti avvenuti solo in Italia negli ultimi mesi, se confrontati con la quasi stagnazione del periodo precedente.

Oggi più che mai i cittadini europei hanno bisogno di semplificare i rapporti intercorrenti con le Pubbliche Amministrazioni dell'Unione. Ma non solo: c'è grande richiesta di interoperabilità tra sistemi nazionali per sfruttare i vantaggi del mercato unico digitale. Tra l'altro, il risparmio si qualifica come punto chiave di questa trasformazione. Se in economia il tempo acquisisce un significato monetario, si può giustamente immaginare come i cittadini, alla luce delle possibilità date dagli strumenti tecnologici, non siano più disposti a passare ore in fila davanti a uno sportello. Al contrario, le persone vogliono riappropriarsi del proprio tempo. Dall'altro lato, il risparmio e l'efficienza sono molto preziosi anche per le Pubbliche Amministrazioni che si trovano di fronte alla difficoltà del taglio della spesa pubblica per tentare di limitare il debito dello Stato.

Per questo c'è bisogno di ripensare integralmente i servizi pubblici: si può parlare infatti di una vera e propria trasformazione digitale. Non basta infatti apportare qualche modifica ai meccanismi attualmente vigenti, ma è necessaria una riorganizzazione generale delle modalità per usufruire dei servizi in rete affinché questi risultino pienamente funzionali e non semplicemente attivi. Inoltre, per realizzare l'obiettivo, tutti i nuovi servizi devono essere offerti preferibilmente in formato digitale sin dalla progettazione, così da evitare inutili duplicazioni e costi

necessari per la conversione dall'analogico al digitale. Attualmente gli utenti nei vari contesti hanno risposto molto bene ai servizi proposti in formato digitale. Gli strumenti attivati sono a loro volta a tratti audaci e all'avanguardia e presentano per questo, data la loro natura versatile, innumerevoli possibilità di applicazione. Avere un'identità digitale potrebbe e dovrebbe consentire di fare praticamente qualsiasi cosa in rete. Gli esempi di Barcellona, Milano e Tallinn sono le testimonianze a favore di questa tesi.

La trasformazione digitale però per essere pienamente effettiva deve essere più di ogni altra cosa universale. Ciò significa che potenzialmente nessuno dovrebbe essere lasciato indietro, e quindi vanno adottate tutte le misure possibili contro il pericolo di esclusione. In particolare, sarà necessario promuovere iniziative diffuse e ricorrenti di alfabetizzazione informatica per coinvolgere le fasce a rischio, e rendere più agevole il reperimento delle informazioni sui siti internet istituzionali. Oltre a questo, se da una parte le eID portano indubbiamente semplificazione, anche il loro stesso funzionamento dovrebbe essere caratterizzato dall'essere user-friendly. Purtroppo molto spesso invece accade che l'identità digitale venga vista a ragione come un ostacolo, e non come il mezzo per eccellenza che permette di accedere ai servizi tipici della cittadinanza digitale. Inoltre, non deve essere lasciato sullo sfondo un punto centrale: gli utenti hanno bisogno di percepire sicurezza nella gestione dei loro dati sensibili, e a questo proposito è richiesto un lavoro costante per garantire la privacy e impedire attacchi informatici. Se i sistemi su cui si basa il funzionamento delle identità digitali non fossero effettivamente sicuri, ci troveremmo davanti a una catastrofe che vedrebbe pubblici dati che per loro natura avrebbero dovuto essere protetti. Su questo è importante impostare un lavoro a livello di rete europea. Infatti, dato che spesso gli attacchi provengono da oltre confine ed evolvono con molta rapidità, si è visto come in materia di cybersicurezza sia molto più efficace sviluppare soluzioni sfruttando la co-creazione.

Concludendo, in più punti è stata evidenziata la portata del cambiamento e i vantaggi dell'uso di una prova certa dell'identità in rete. Un'unica identità digitale

per accedere a qualsiasi servizio della Pubblica Amministrazione è un progetto in atto da ormai vent'anni nei diversi Stati europei con differenti risultati e risposte. La piena realizzazione sicuramente non avverrà domani o dopo domani, e le difficoltà non sono certo finite. Tuttavia, la spinta all'innovazione è così forte che ci si aspetta grandi risultati già nei prossimi anni. Che sia giunto o meno il tempo della cittadinanza digitale, non è ancora ben chiaro, ma appare evidente quanto ormai le identità digitali abbiano spalancato la porta verso questa direzione. In base all'analisi svolta però, si può immaginare ragionevolmente come questo cambiamento sia ben più vicino di quanto ci si aspetti.

Fonti

[1] *Codice dell'amministrazione digitale*, 13 febbraio 2020, da https://docs.italia.it/media/pdf/codice-amministrazione-digitale-docs/v2018-09-28/codice-amministrazione-digitale-docs.pdf

[2] 2014/910/EU, 23 luglio 2014, *Regulation (EU) 910/2014 of the European Parliament and of the council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, da http://data.europa.eu/eli/reg/2014/910/oj

[3] COLACICCO C., 30 dicembre 2019, *Firme elettroniche, tutte le tipologie alla luce del Regolamento eIDAS*, da https://www.agendadigitale.eu/documenti/firme-elettroniche-tutte-le-tipologie-alla-luce-del-regolamento-eidas/

[4] *Firme e Sigilli Elettronici. Analisi comparativa delle varie tipologie presenti nella normativa nazionale e comunitaria*, dicembre 2019, da https://www.agid.gov.it/sites/default/files/repository_files/tipologie_di_firme_e_sigilli_elettronici_v1_dicembre_2019.pdf

[5] La Posta Elettronica Certificata, 20 luglio 2020, da https://www.legalmail.it/info/pec-posta-elettronica-certificata.php

[6] *Il domicilio digitale: PEC e servizi di recapito certificato*, 9 aprile 2020, da https://www.agendadigitale.eu/documenti/il-domicilio-digitale-pec-e-servizi-di-recapito-certificato/

[7] MANCA G., 30 gennaio 2018, *Servizio elettronico di recapito certificato, cos'è e perché potrebbe pensionare la Pec*, da https://www.agendadigitale.eu/cittadinanza-digitale/servizio-elettronico-recapito-certificato-cose-perche-pensionare-la-pec/

[8] Guida alla Marcatura Temporale: che cos'è e come funziona, 28 luglio 2020, da https://www.marchetemporali.com/marcatura-temporale.php

[9] 2015/1501/EU, 8 settembre 2015, *Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, da http://data.europa.eu/eli/reg_impl/2015/1501/oj

[10] 2016/679/EU, 2016, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, da http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

[11] 2018/1724/EU, 2 ottobre 2018, *Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012*, da http://data.europa.eu/eli/reg/2018/1724/oj

[12] 2019/881/EU, 2019, *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*, da http://data.europa.eu/eli/reg/2019/881/oj

[13] ETSI, 27 giugno 2020, da https://www.etsi.org

[14] ISO, 29 giugno 2020, da https://www.iso.org/home.html

[15] Agenzia per l'Italia digitale (AgID), 25 luglio 2020, da https://www.agid.gov.it/it

[16] *Vigilanza sui soggetti qualificati o accreditati (QTS, PEC, Conservazione, SpID). Rapporto di riepilogo*, gennaio-dicembre 2019, da https://www.agid.gov.it/sites/default/files/repository_files/sv_dr01_rapporto_di_riepilogo_2019.pdf

[17] *Regolamento concernente le procedure interne all'Agenzia per l'Italia digitale aventi rilevanza esterna, finalizzate allo svolgimento nella fase di prima applicazione dei compiti previsti dall'articolo 17, comma 1-quater del Codice dell'Amministrazione digitale, relativi al difensore civico per il digitale*, 12 febbraio 2018, da https://www.agid.gov.it/sites/default/files/repository_files/37_-_dt_dg_n._37_-_12_feb_2018_-_approvazione_regolamento_difensorecivicodigitale_1.pdf

[18] *Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021*, da https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2019_-_2021_allegati20190327.pdf

[19] *Piano nazionale innovazione 2025*, 13 febbraio 2020, da https://docs.italia.it/media/pdf/piano-nazionale-innovazione-2025-docs/stabile/piano-nazionale-innovazione-2025-docs.pdf

[20] Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022, luglio 2020, da https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pa_2020_2022.pdf

[21] *Linee guida sulla formazione, gestione e conservazione dei documenti informatici*, 13 febbraio 2020, da https://docs.italia.it/media/pdf/lg-documenti-informatici-docs/bozza/lg-documenti-informatici-docs.pdf

[22] MANCA G., 18 ottobre 2019, *Linee Guida di AgID sui documenti informatici: novità e punti chiave*, da https://www.agendadigitale.eu/documenti/linee-guida-di-agid-sui-documenti-informatici-novita-e-punti-chiave/

[23] SAVINO N., 30 ottobre 2019, *Linee guida Agid documenti informatici, che cambia*, da https://www.agendadigitale.eu/documenti/linee-guida-agid-documenti-informatici-che-cambia/

[24] *Indice di digitalizzazione dell'economia e della società (DESI) 2020*, 2020, da https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66946

[25] SPID - Sistema Pubblico di Identità Digitale, 6 agosto 2020, da https://www.agid.gov.it/it/piattaforme/spid

[26] Il progetto FICEP - First Italian Crossborder eIDAS Proxy, 25 giugno 2020, da https://www.agid.gov.it/it/piattaforme/eidas/progetto-ficep

[27] Richiedi SPID, 9 luglio 2020, da https://www.spid.gov.it/richiedi-spid

[28] DRAGONI G., GASTALDI L. & PORTALE V., 5 agosto 2020, *SPID (Sistema Pubblico di Identità Digitale), cos'è, a cosa serve e come creare un account*, da https://www.agendadigitale.eu/cittadinanza-digitale/a-che-punto-e-il-sistema-pubblico-dell-identita-digitale-e-a-che-serve/

[29] *Mezzi d'identificazione elettronica riconosciuti a livello statale (eID)*, 2 febbraio 2017, da https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwinz8D9hJHrAhXR_KQKHeqFD5gQFjAFegQIBhAB&url=https%3A%2F%2Fwww.ejpd.admin.ch%2Fdam%2Ffedpol%2Fit%2Fdata%2Fpass-id%2Fkonsultation%2Fkonzept-i.pdf.download.pdf%2Fkonzept-i.pdf&usg=AOvVaw3sZqGtGWq8GXdri8spMecZ

[30] *Linee guida per il rilascio dell'identità digitale per uso professionale*, novembre 2019, da https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_identita_digitale_per_uso_professionale_v.1.0_0.pdf

[31] PIUNNO S., PAOLINI V., 4 aprile 2019 , *I vantaggi della Carta d'Identità elettronica, che con la nuova "Agenda CIE", sarà più semplice richiedere*, da https://medium.com/team-per-la-trasformazione-digitale/carta-identita-elettronica-come-richiederla-agenda-cie-prenotazioni-appuntamento-in-comune-7dd104e8ee75

[32] Caratteristiche del documento, 16 agosto 2020, da https://www.cartaidentita.interno.gov.it/caratteristiche-del-documento/

[33] LONGO A., SAGGINI P., 19 febbraio 2020, *Carta d'Identità Elettronica (CIE): cos'è, come funziona, quanto costa e come ottenerla*, da https://www.agendadigitale.eu/cittadinanza-digitale/carta-didentita-elettronica-a-cosa-serve-quanto-costa-e-come-ottenerla/

[34] Cosa sono PIN e PUK e come utilizzarli, 16 agosto 2020, da https://www.cartaidentita.interno.gov.it/cosa-pin-puk-utilizzarli/

[35] PISANU N., 29 luglio 2019, *CNS: cos'è e come utilizzare la Carta nazionale dei servizi (guida completa 2019)*, da https://www.agendadigitale.eu/documenti/cns-cose-e-come-utilizzare-la-carta-nazionale-dei-servizi-guida-completa-2019/

[36] ANPR - Anagrafe Nazionale della Popolazione Residente, 18 agosto 2020, da https://www.agid.gov.it/it/piattaforme/anagrafe-nazionale-popolazione-residente

[37] SAGGINI P., 28 luglio 2020, *ANPR, il quadro completo: i subentri dei Comuni, le sfide, vantaggi e le novità del DL Semplificazione*, da https://www.agendadigitale.eu/cittadinanza-digitale/anagrafe-unica/anpr-sta-andando-subentri-dei-comuni-le-norme-portale-del-cittadino/

[38] Anagrafe Nazionale della Popolazione Residente, 18 agosto 2020, da https://innovazione.gov.it/it/progetti/anpr/

[39] Guida ad ANPR, 18 agosto 2020, da https://www.anpr.interno.it/portale/guida-anpr?p_p_id=56_INSTANCE_FM16LyuxR7MD&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1

[40] Cos'è pagoPA, 18 agosto 2020, da https://www.pagopa.gov.it/it/pagopa/

[41] DE PICCOLI I., 14 maggio 2020, *PagoPA, cos'è, come funziona e come pagare servizi pubblici online*, da https://www.agendadigitale.eu/cittadinanza-digitale/pagopa-funziona-punto-cio-bisogna-sapere/

[42] Pagamenti digitali, 18 agosto 2020, da https://innovazione.gov.it/it/progetti/pagopa/

[43] PagoPA - Il servizio di pagamento verso la Pubblica Amministrazione, 18 agosto 2020, da https://designers.italia.it/progetti/pagopa/#

[44] TUMIETTO D., 23 aprile 2019, *Fatturazione elettronica obbligatoria 2020: cos'è, come funziona, come fare, esoneri e normativa (tra privati, PA e B2B)*, da https://www.agendadigitale.eu/documenti/fatturazione-elettronica/fatturazione-elettronica-tra-privati-quale-futuro-ci-attende/

[45] *La fattura elettronica e i servizi gratuiti dell'Agenzia delle Entrate*, 4 ottobre 2018, da https://www.agenziaentrate.gov.it/portale/documents/20143/451290/guida+FE+e+servizi+AdE+in+pdf_Guida_La+fattura_elettronica_e_i_servizi_g_10082020.pdf/035e38b3-2309-3335-f135-6e6010252e7a

[46] Fatturazione elettronica: oltre due miliardi di fatture emesse in un anno, 24 aprile 2020, da https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/04/24/fatturazione-elettronica-oltre-due-miliardi-fatture-emesse-anno

[47] Fatturazione elettronica, 21 agosto 2020, da https://www.agid.gov.it/it/piattaforme/fatturazione-elettronica

[48] RUGGIERO G., 6 giugno 2020, *L'app IO dei servizi pubblici in Italia: come si scarica, come si usa e il suo senso strategico*, da https://www.agendadigitale.eu/cittadinanza-digitale/lapp-io-pronta-al-lancio-cosi-i-servizi-pubblici-saranno-a-portata-di-smartphone/

[49] La Roadmap di sviluppo di IO, 22 agosto 2020, da https://io.italia.it/roadmap/#nextsteps

[50] TASSI R., DE SANTI M., 25 settembre 2019, *Come essere parte del progetto IO: una guida per gli enti pubblici*, da https://medium.com/team-per-la-trasformazione-digitale/progetto-io-guida-per-gli-enti-pubblici-integrazione-servizi-pubblica-amministrazione-smartphone-cittadini-f290306a611a

[51] Il fascicolo Sanitario Elettronico (FSE), 25 agosto 2020, da https://www.fascicolosanitario.gov.it/il-fascicolo-sanitario-elettronico

[52] Sanità digitale, 25 agosto 2020, da https://www.agid.gov.it/it/piattaforme/sanita-digitale

[53] COLLICELLI C. et al., luglio 2016, *Le condizioni per lo sviluppo della Sanità Digitale: scenari Italia-UE a confronto*, da https://www.sanita24.ilsole24ore.com/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANO_SANITA/Online/_Oggetti_Correlati/Documenti/2016/07/06/Sanita_digitale_2016.pdf?uuid=ADs36Io

[54] Fascicolo Sanitario elettronico: adesso unico con SPID. E interoperabilità tra le Regioni, 25 agosto 2020, da https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/09/04/fascicolo-sanitario-elettronico-accesso-unico-spid-interoperabilita-regioni

[55] eHealth - Sanità digitale, 25 agosto 2020, da http://www.salute.gov.it/portale/temi/p2_4.jsp?lingua=italiano&tema=Ricerca%20e%20innovazione&area=eHealth

[56] Presentazione delle iniziative di eHealth in Italia, 25 agosto 2020, da http://www.salute.gov.it/portale/temi/p2_6.jsp?lingua=italiano&id=2509&area=eHealth&menu=iniziative

[57] Cloud della PA, 31 gennaio 2020, da https://www.agid.gov.it/it/infrastrutture/cloud-pa

[58] *Il modello di Cloud della PA*, 13 febbraio 2020, da https://docs.italia.it/media/pdf/cloud-docs/stabile/cloud-docs.pdf

[59] *Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione, 24 maggio 2012*, da https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/sistemi_cloud_pa.pdf

[60] *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, 28 giugno 2012, da https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/raccomandazioni_cloud_e_pa_-_2.0_0.pdf

[61] NICOTRA M., 25 giugno 2019, *Tutta la PA in Cloud? Ecco i passaggi e le competenze necessari*, da https://www.agendadigitale.eu/infrastrutture/tutta-la-pa-in-cloud-ecco-i-passaggi-e-le-competenze-necessari/

[62] PUGGIONI S. (a cura di), giugno 2016, *E-public procurement. Il ruolo delle Ict nell'innovazione del processo di approvvigionamento della Pa*, da https://st.ilsole24ore.com/temi-ed-eventi/qelpa/E-Public%20Procurement.pdf

[63] E-Procurement, 19 agosto 2020, da https://www.agid.gov.it/index.php/it/piattaforme/procurement

[64] *Rapporto AGID sulla Spesa ICT nella Sanità territoriale italiana*, aprile 2019-ottobre 2019, da https://www.agid.gov.it/sites/default/files/repository_files/rapporto_agid_sulla_spesa_ict_nella_sanita_territoriale_italiana.pdf

[65] The Digital Economy and Society Index (DESI), 25 agosto 2020, da https://ec.europa.eu/digital-single-market/en/desi

[66] Il monitoraggio dei progetti di trasformazione digitale, 25 agosto 2020, da https://avanzamentodigitale.italia.it/it

[67] SPID - Avanzamento trasformazione digitale, 2 ottobre 2020, da https://avanzamentodigitale.italia.it/it/progetto/spid

[68] Carta di Identità Elettronica - I dati, 2 ottobre 2020, da https://innovazione.gov.it/it/progetti/cie/

[69] ANPR - Avanzamento trasformazione digitale, 2 ottobre 2020, da https://avanzamentodigitale.italia.it/it/progetto/anpr

[70] PagoPA - Avanzamento trasformazione digitale, 2 ottobre 2020, da https://avanzamentodigitale.italia.it/it/progetto/pagopa

[71] Dashboard pagoPA, 2 ottobre 2020, da https://www.pagopa.gov.it/it/pagopa/dashboard/

[72] FSE - Avanzamento trasformazione digitale, 2 ottobre 2020, da https://avanzamentodigitale.italia.it/it/progetto/fse

[73] I numeri dell'app IO, 2 ottobre 2020, da https://io.italia.it/dashboard/

[74] LEITOLD H., ZWATTENDORFER B, 2011, *STORK: Architecture, Implementation and Pilots*. In POHLMANN N. et al, ISSE 2010 Securing Electronic Business Processes, Vieweg+Teubner, da https://link.springer.com/content/pdf/10.1007%2F978-3-8348-9788-6.pdf

[75] LEITOLD H., 2011, *Challenges of eID Interoperability: The STORK project*. In: FISCHER-HÜBNER S. et al, Privacy and Identity Management for Life, Springer, da https://link.springer.com/content/pdf/10.1007%2F978-3-642-20769-3.pdf

[76] *STORK 2.0 Pilots to Improve Cross-Border Online Services for EU Citizens*, 30 marzo 2015, da https://chronicle.lu/category/living-in-luxembourg/10895-stork-2-0-pilots-to-improve-cross-border-online-services-for-eu-citizens

[77] RIBEIRO C. et al., 5 luglio 2017, *STORK: a real, heterogeneous, large-scale eID management system*, International Journal of Information Security 17, 569-585 (2018), da https://link.springer.com/content/pdf/10.1007/s10207-017-0385-x.pdf

[78] KOULOLIAS V., 9 gennaio 2013, *STORK 2.0 - Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0)*, da https://joinup.ec.europa.eu/collection/secure-identity-across-borders-linked-stork/document/stork-20-secure-identity-across-borders-linked-20-stork-20

[79] Secure Identity Across Borders Linked, 29 agosto 2020, da https://cordis.europa.eu/project/id/224993

[80] Secure idenTity acrOss boRders linKed 2.0, 29 agosto 2020, da https://cordis.europa.eu/project/id/297263

[81] The Once Only Principle Project, 28 agosto 2020, da https://cordis.europa.eu/project/id/737460

[82] TOOP website, 28 agosto 2020, da https://www.toop.eu

[83] KRIMMER R. et al., dicembre 2017, *The Once-Only Principle Project. Position Paper on Definition of OOP and Situation in Europe (updated version)*, da https://www.researchgate.net/profile/Aleksandrs_Cepilovs2/project/TOOP-The-Once-Only-Principle-Project/attachment/5a4dec004cde266d587ff30c/AS:

5 7 9 0 0 1 5 1 8 1 8 2 4 0 0 @ 1 5 1 5 0 5 6 1 2 7 9 5 5 / d o w n l o a d / D2.14_Position_paper_OOP_update.pdf?context=ProjectUpdatesLog

[84] SCOOP4C website, 31 agosto 2020, da https://scoop4c.eu

[85] WIMMER M. A., MARINOV B., 2017, *SCOOP4C: Reducing administrative burden for citizens through once-only - vision & challenges*, da https://www.scoop4c.eu/sites/default/files/2017-05/Wimmer%20MW%20BM%20SCOOP4C_p159_ES_0.pdf

[86] Implementation of TOOP solution. Italian Success Story, 31 agosto 2020, da https://toop.eu/sites/default/files/italian-v2.pdf

[87] TOOP Pilot Testing, 31 agosto 2020, da https://toop.eu/sites/default/files/TOOP_Pilot_testing_final2.pdf

[88] KALVET T. et al., aprile 2018, *Cross-border e-Government Services in Europe: Expected benefits, Barriers and Drivers of the Once-Only Principle*, da https://dl.acm.org/doi/abs/10.1145/3209415.3209458

[89] TEPANDI J. et al., 19 novembre 2019, *Towards a Cross Border Reference Architecture for the Once-Only Principle in Europe: An Enterprise Modeling Approach*, da https://link.springer.com/chapter/10.1007/978-3-030-35151-9_7

[90] KRIMMER R. et al., giugno 2017, *Exploring and Demonstrating the Once-Only Principle: A European Perspective*, da https://dl.acm.org/doi/abs/10.1145/3085228.3085235

[91] GRANDRY E. et al., settembre 2018, *The Once-Only Principle Project. Generic Federated OOP Architecture (3rd version)*, da https://www.toop.eu/sites/default/files/D23_Generic_Federated_OOP_Architecture_3rd_version.pdf

[92] Stakeholder community for once-only principle: Reducing administrative burden for citizens, 31 agosto 2020, da https://cordis.europa.eu/project/id/737492/it

[93] *Deliverable D 1.1: Vision of the once-only principle for citizens, including key enablers and major barriers*, agosto 2017, da https://scoop4c.eu/sites/default/files/2018-01/SCOOP4C_D1.1.pdf

[94] *Deliverable 4.1: Gap analysis report of challenges, needs and benefits of the OOP4C analysis*, maggio 2019, da https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c486b89e&appId=PPGMS

[95] ANNEX D3.2. White Paper: The POSEID-ON Blockchain-based Platform meets the "right to be forgotten", 2020, da https://www.poseidon-h2020.eu/wp-content/uploads/2020/06/Annex-D3.2_White-paper_POSEIDON_FinalReview-clean.pdf

[96] SILVA P. et al., 2020, *Risk Management and Privacy Violation Detection in the PoSeID-on Data Privacy Platform*, da https://link.springer.com/content/pdf/10.1007/s42979-020-00198-9.pdf

[97] *PoSeID-on. Deliverable 3.1. PoSeID-on blockchain - Interim implementation*, 30 luglio 2019, da https://www.poseidon-h2020.eu/wp-content/uploads/2019/08/D3.1_final-version_POSEIDON_v10.pdf

[98] BAGNATO A. et al., *2019, Workshop on privacy Challenges in Public and Private Organizations*, da http://www.eurecom.fr/en/publication/6141/download/sec-publi-6141.pdf

[99] PoSeID-on. Deliverable 2.1 - Use cases analysis and user scenarios, 27 dicembre 2017, da https://www.poseidon-h2020.eu/wp-content/uploads/2019/08/PoSeID-on_D2.1-Use-cases-analysis-and-user-scenarios-v1.1.pdf

[100] Protection and control of Secured Information by means of a privacy enhanced Dashboard, 28 agosto 2020, da https://cordis.europa.eu/project/id/786713

[101] PoSeID-on website, 28 agosto 2020, da https://www.poseidon-h2020.eu

[102] DE CARVALHO R. M. et al., 27 giugno 2020, *Protecting Citizens' Personal Data and privacy: Joint Effort from GDPR EU Cluster Research Projects*, da https://link.springer.com/content/pdf/10.1007/s42979-020-00218-8.pdf

[103] ARRIGO F., 29 aprile 2019, *Blockchain e smart contract: funzionamento e applicazioni*, da https://www.altalex.com/documents/news/2019/04/29/tecnologia-blockchain-e-smart-contract

[104] BELLINI M., 20 luglio 2020, *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia*, da https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

[105] *eGovernment Benchmark 2019. Empowering Europeans through trusted digital public services*, da https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62298

[106] *e-ESTONIA. e-Governance in Practice*, 2016, da https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf

[107] *Estonia - the Digital Republic Secured by Blockchain*, da https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

[108] *Digital Economy and Society Index (DESI) 2020. Estonia*, 2020, da https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66911

[109] KASTTEL R., MERGEL I., 2019, *Estonia's Digital Transformation*, in COMPTON M. E., 'T HART P. (a cura di), Great Policy Successes, Oxford University press, pagine 143-160, da https://library.oapen.org/bitstream/handle/20.500.12657/23594/9780198843719.pdf?sequence=1#page=158

[110] ANTHES G., maggio 2015, *Estonia: a Model for e-government*, da https://dl.acm.org/doi/abs/10.1145/2754951

[111] MARTENS T., 2010, *Electronic identity management in Estonia between market and state governance*, da https://link.springer.com/content/pdf/10.1007/s12394-010-0044-0.pdf

[112] E-identity. Smart-ID, 11 settembre 2020, da https://e-estonia.com/solutions/e-identity/smart-id

[113] TSAP V. et al., 2020, *eID Public Acceptance in Estonia: towards Understanding the Citizen*, da https://dl.acm.org/doi/10.1145/3396956.3397009

[114] VAN DE POLL M., 18 febbraio 2020, *The History of Digital Identity in Estonia*, da https://cyber.ee/blog/2020/02-18/

[115] Tallinnovation. Smart Tallinn Brochure, da https://www.tallinn.ee/est/g2613s130637

[116] PLANTERA F., maggio 2018, *Tallinn - the smart capital of a digital nation*, da https://e-estonia.com/tallinn-smart-capital-digital-nation/

[117] KOTKA T. et al., 2015, *Estonian e-Residency: Redefining the National-State in the Digital Era*, da https://www.politics.ox.ac.uk/materials/publications/14883/workingpaperno3kotkavargaskorjus.pdf

[118] *How Estonia is Pioneering the Digital Identity Space*, giugno 2019, da https://medium.com/metadium/how-estonia-is-pioneering-the-digital-identity-space-4008c709fbb8

[119] VATTER O., settembre 2019, *Why Estonia pioneered digital identity*, da https://www.techradar.com/news/why-estonia-pioneered-digital-identity

[120] Comune di Tallinn official website, 11 settembre 2020, da https://www.tallinn.ee/eng/

[121] Tallinn Innovation official website, 11 settembre 2020, da https://www.tallinn.ee/eng/tallinnovations/

[122] Tallinn Dashboard official website, 11 settembre 2020, da http://gis.tallinn.ee/portal/apps/opsdashboard/index.html#/355a2c1bd19d4f47b554ec4bfd82a666

[123] e-identity, 11 settembre 2020, da https://e-estonia.com/solutions/e-identity/

[124] We have build a digital society and we can show you how, 11 settembre 2020, da https://e-estonia.com

[125] *E-Government closer to the people*, 2019 da http://dilersur.com/wp-content/uploads/2019/04/e-book-final-28.04.2019-1.pdf

[126] BARRERA-BARRERA R. et al., aprile 2019, *Explanatory factors of the preference and use of electronic administration in Spain*, da https://www.scielo.br/scielo.php?pid=S0034-76122019000200349&script=sci_arttext&tlng=en

[127] ¿Qué es Cl@ve?, 17 settembre 2020, da https://clave.gob.es/clave_Home/clave/queEs.html

[128] *eGovernment in Spain*, febbraio 2016, da https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment%20in%20Spain%20-%20February%202016%20-%2018_0_4_00.pdf

[129] *eGovernment in Spain*, 2018, da https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Spain_December_2018_v2.00.pdf

[130] Barcelona Digital Government: Open, Agile and Participatory, 17 settembre 2020, da https://ajuntament.barcelona.cat/digital/en/blog/barcelona-digital-government-open-agile-and-participatory

[131] Open-source software, 17 settembre 2020, da https://ajuntament.barcelona.cat/digital/en/digital-transformation/technology-for-a-better-government/open-source-software

[132] CALZADA I., settembre 2018, *(Smart) Citizens from Data Providers to Decision-Makers? The Case Study of Barcelona*, da https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiTsdHGpObrAhWOjKQKHYXdDCw4KBAWMAR6BAgGEAE&url=https%3A%2F%2Fwww.mdpi.com%2F2071-1050%2F10%2F9%2F3252%2Fpdf&usg=AOvVaw2CJXRN6ZhbB3unpqNUDK35

[133] *Rejuvenating Barcelona with digital technologies*, gennaio 2017, da https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Barcelona%20v1.pdf

[134] Open Data BCN official website, 17 settembre 2020, da https://opendata-ajuntament.barcelona.cat/en/

[135] Barcelona digital city. Putting technology at the service of people (2015-2019), da https://ajuntament.barcelona.cat/digital/sites/default/files/pla_barcelona_digital_city_in.pdf

[136] Data Commons Barcelona official website, 17 settembre 2020, da https://datacommons.barcelona/en/

[137] PREVILLE P., 13 novembre 2019, *How Barcelona is leading a new era of digital democracy*, da https://medium.com/sidewalk-talk/how-barcelona-is-leading-a-new-era-of-digital-democracy-4a033a98cf32

[138] Institut Municipal d'Informàtica (Barcelona), 14 settembre 2020, da https://ajuntament.barcelona.cat/imi/es

[139] NOORI N. et al., maggio 2020, *Classifying Pathways for Smart City Development: Comparing Design, governance and Implementation in Amsterdam, Barcelona, Dubai, and Abu Dhabi*, da https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjSmuWLqObrAhVH_KQKHcQ_DNUQFjAGegQIBxAB&url=https%3A%2F%2Fwww.mdpi.com%2F2071-1050%2F12%2F10%2F4030%2Fpdf&usg=AOvVaw3Q8U2M1UaWm62JfcfGhVss

[140] Sede electrónica. Ajuntament de Barcelona, 12 settembre 2020, da https://seuelectronica.ajuntament.barcelona.cat/es/

[141] Barcelona promotes digital services, 17 settembre 2020, da https://ajuntament.barcelona.cat/digital/en/noticia/barcelona-promotes-digital-services-2_712356

[142] Oficina virtual de Trámites. Lista alfabética de trámites realizables electrónicamente, 12 settembre 2020, da https://seuelectronica.ajuntament.barcelona.cat/oficinavirtual/es/all-search-result

[143] Métodos de identificación, 17 settembre 2020, da https://seuelectronica.ajuntament.barcelona.cat/oficinavirtual/es?vo=active

[144] Mobile ID official website, 17 settembre 2020, da https://www.mobileid.cat/es/

[145] *Sociedad Digital en España 2018*, 2018, da https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjOy_byi-jrAhWM-KQKHY2hAHQQFjARegQICBAB&url=https%3A%2F%2Fadministracionelectronica.gob.es%2Fpae_Home%2Fdam%2Fjcr%3Aefe8b497-09fb-4c50-a3af-8e156c69b84f%2FSociedad_Digital_Espana_2018.pdf&usg=AOvVaw0OnjwryZ_jLTYuMUh7PK1b

[146] *Digital Economic and Society Index (DESI) 2020. Spain*, 2020, da https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66930

[147] ZEFFERER T., *E-government services in Europe - a comparison of seven countries*, da https://www.vodafone-institut.de/wp-content/uploads/2015/09/VFI_eGovServices_EN.pdf

[148] PARTEKA E., REZENDE A. D., 2018, *Digital planning of the city of Barcelona and its relations with the strategic digital city*, da https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-27242018000400054

[149] Apps municipales, 17 settembre 2020, da https://ajuntament.barcelona.cat/apps/es/mobile-id-identidad-digital-en-el-movil

[150] Barcelona Digital City, 17 settembre 2020, da https://ajuntament.barcelona.cat/digital/en/about-us

[151] *Barcelona: smart city revolution in progress*, 26 ottobre 2017, da https://www.ft.com/content/6d2fe2a8-722c-11e7-93ff-99f383b09ff9

[152] Certificados y sistemas de firma electrónica, 17 settembre 2020, da https://seuelectronica.ajuntament.barcelona.cat/es/certificados-y-sistemas-de-firma-electronica

[153] ICity Rank 2019: Milano, Firenze e Bologna sono le città più smart d'Italia, 26 novembre 2019, da https://www.forumpa.it/citta-territori/icity-rank-2019-milano-firenze-e-bologna-sono-le-citta-piu-smart-ditalia/

[154] Smart City: Milano, 18 settembre 2020, da https://smartcityweb.net/smartcities/milano

[155] Linee guida Milano smart city, maggio 2014, da http://economiaelavoro.comune.milano.it/sites/default/files/2019-02/milano%20smart%20city%20-%20linee%20guida.pdf

[156] Trasformazione Digitale, 17 settembre 2020, da https://www.comune.milano.it/aree-tematiche/trasformazione-digitale

[157] La Vision di Milano Digitale, 2020, da https://www.comune.milano.it/documents/20126/128206432/Piano+di+trasformazione+digitale.pdf/dd03211d-1a95-b528-778b-5a84dc3519f4?t=1595496672278

[158] Innovazione. Comune e Camera di commercio insieme per la diffusione dei servizi digitali, 17 settembre 2020, da https://www.comune.milano.it/-/innovazione.-comune-e-camera-di-commercio-insieme-per-la-diffusione-dei-servizi-digitali

[159] Milano Digital week. È disponibile l'app del Fascicolo del cittadino, 29 maggio 2020, da https://www.comune.milano.it/-/milano-digital-week.-e-disponibile-l-app-del-fascicolo-del-cittadino

[160] Servizi online Comune di Milano, 8 settembre 2020, da https://www.comune.milano.it/servizi?p_p_id=ricerca_INSTANCE_D7SF4dIAlP3V&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_ricerca_INSTANCE_D7SF4dIAlP3V_searchText=&_ricerca_INSTANCE_D7SF4dIAlP3V_categoryId=&_ricerca_INSTANCE_D7SF4dIAlP3V_firstLanding=false&_ricerca_INSTANCE_D7SF4dIAlP3V_sortBy=piuVisti&_ricerca_INSTANCE_D7SF4dIAlP3V_servizioOnline=true&_ricerca_INSTANCE_D7SF4dIAlP3V_restrictCategoryId=0&_ricerca_INSTANCE_D7SF4dIAlP3V_cur=1&_ricerca_INSTANCE_D7SF4dIAlP3V_resetCur=false

[161] Milano 2020. La risposta digitale all'emergenza, 2020, da https://www.comune.milano.it/documents/20126/128206432/Milano+2020+-+La+risposta+digitale+all%27emergenza.pdf/8ca09372-7c7c-4787-caa1-908afdbc3101?t=1596120552251

[162] Servizi on-line Comune di Tallinn, 11 settembre 2020, da https://www.tallinn.ee/teenused?filter_otsing_teenus_fraas=&laiendatud_otsing=&filter_otsing_teenus_valdkond=0&filter_otsing_teenus_menetluseliik=7&filter_otsing_teenus_klass=0&filter_otsing_teenus_asutus=&filter_otsing_teenus_taht=

[163] Milano Smart City Conference, 18 settembre 2020, da https://www.smartbuildingitalia.it/smart-city-conference/

[164] Linee guida Milano Smart City (website), 18 settembre 2020, da https://economiaelavoro.comune.milano.it/progetti/linee-guida-milano-smart-city

[165] COCCO R., 16 luglio 2019, *Cocco: "Tutte le sfide della semplificazione a Milano"*, da https://www.agendadigitale.eu/cittadinanza-digitale/cocco-tutte-le-sfide-della-semplificazione-a-milano/

[166] Fascicolo digitale del Cittadino, 17 settembre 2020, da https://www.comune.milano.it/servizi/fascicolo-del-cittadino

[167] Milano 2020. Digital Care, 2020, da https://www.comune.milano.it/documents/20126/128206432/Digital+Care.pdf/79eee442-869c-a90d-df63-813da384ce96?t=1595496581028

[168] *Tallin was rewarded with the International Smart City Award*, 3 dicembre 2019, da https://www.tallinn.ee/eng/Uudis-Tallinn-was-rewarded-with-the-International-Smart-City-Award

[169] *The three pillars of the digital transformation in Tallinn*, 12 settembre 2019, da https://www.theagilityeffect.com/en/case/the-three-pillars-of-the-digital-transformation-in-tallinn/

[170] NIELSEN M. M., 2019, *Tackling identity management, service delivery, and social security challenges: technology trends and partnership models*, da https://collections.unu.edu/eserv/UNU:7321/p001-Meyerhoff-Nielsen.pdf

[171] ALEXOPOULOS C. et al., 2019, *Benefits and Obstacles of Blockchain Applications in e-Government*, da http://128.171.57.22/bitstream/10125/59773/0333.pdf

[172] *Blockchain and digital identity*, 2019, da https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

[173] *eIDAS Compliant eID Solutions. Security Considerations and the Role of ENISA*, 2020, da https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/at_download/fullReport

[174] *Trust services security incidents 2019. Annual Analysis Report*, 2020, da https://www.enisa.europa.eu/publications/trust-services-security-incidents-2019-annual-analysis-report/at_download/fullReport

[175] THIRD A. et al., agosto 2018, *Government services and digital identity*, da https://www.eublockchainforum.eu/sites/default/files/research-paper/20180801_government_services_and_digital_identity.pdf?width=1024&height=800&iframe=true

[176] Challenges encountered in the use of electronic services in the public administration from EU Member States. Comparative study, 2019, da https://www.eupan.eu/wp-content/uploads/2019/06/RO-EUPAN-Comparative-Study-Public-Electronic-Services.pdf

[177] HAYAT A. et al., 2005, *Identifying Obstacles in moving towards an Interoperable Electronic Identity Management System*, da https://pdfs.semanticscholar.org/4f2e/fd2ec26553530fa7e09d64b153fe52db011294.pdf?_ga=2.263155788.1118214068.1599546720-1991192532.1599128351

[178] LUTAAYA M., 2019, *Me, myself, and I: towards usable, privacy-preserving, fraud-resistant digital identity services for smartphone users*, da https://curve.carleton.ca/system/files/etd/84af1b29-da57-498c-916b-427b61909ad0/etd_pdf/26bf700627 7e111cd615947cd662ff5a/lutaaya-memyselfandidtowardsusableprivacypreserving.pdf

[179] ATZORI M., 2017, *Blockchain Governance and the Role of Trust Service Providers: The TrustedChain® Network*, da https://jbba.scholasticahq.com/article/3553.pdf

[180] *Conformity assessment of trust service providers. Technical guidelines on trust services*, dicembre 2017, da https://www.enisa.europa.eu/publications/tsp-conformity-assessment/at_download/fullReport

[181] Cybersecurity Incident Report and Analysis System - Visual Analysis Tool, 29 settembre 2020, da https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

[182] *E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development. With addendum on COVID-19 Response*, da https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf

[183] *Global Cybersecurity Index (GCI) 2018*, 2019, da https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[184] eGovernment & Digital Public Services, 27 settembre 2019, da https://ec.europa.eu/digital-single-market/en/policies/egovernment

[185] European eGovernment Action Plan 2016-2020, da https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020

[186] Ministerial Declaration on eGovernment - the Tallinn Declaration, 29 settembre 2019, da https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

[187] *Ministerial Declaration on eGovernment approved in Malmö*, 18 novembre 2009, da https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf

[188] MARCELLINO G., 31 luglio 2020, *Identità digitali, le novità del decreto Semplificazioni e come farle funzionare*, da https://www.agendadigitale.eu/cittadinanza-digitale/identita-digitale/identita-digitali-le-novita-del-decreto-semplificazioni-ora-comunicarle-a-cittadini-pa-e-imprese/

[189] eGovernment in local and regional administrations: guidance, tools and funding for implementation, 23 ottobre 2017, da https://ec.europa.eu/digital-single-market/en/news/egovernment-local-and-regional-administrations-guidance-tools-and-funding-implementation

[190] DE PIETRO L., SANNA ARTIZZU M. A., dicembre 2017, *Il Percorso dell'Agenda Digitale Italiana*, da http://egov.formez.it/sites/all/files/agenda_digitale_italiana.pdf

[191] TC CYBER Roadmap, 28 luglio 2020, da https://www.etsi.org/cyber-security/tc-cyber-roadmap

[192] BROOKSON C. et al., dicembre 2016, *Tackling the Challenges of Cyber Security*, da https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp18_CyberSecurity_Ed1_FINAL.pdf

[193] CUCCINIELLO M. et al, 2018, *Management pubblico*, capitolo 20, Milano, EGEA

[194] The cyber secrets, gennaio-febbraio 2019, da https://www.iso.org/files/live/sites/isoorg/files/news/magazine/ISOfocus%20(2013-NOW)/en/2019/ISOfocus_132/ISOfocus_132_en.pdf

[195] Study on the use of Electronic Identification (eID) for the European Citizens' Initiative. Final Assessment Report, settembre 2017, da https://europa.eu/citizens-initiative/sites/default/files/2019-12/Study%20on%20the%20use%20of%20electronic%20identification%20%28eID%29%20-%20final%20report.pdf

[196] Trends in electronic identification. An overview, settembre 2018, da https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihMCg3L3rAhUQqaQKHWv5AGIQFjADegQIAxAB&url=https%3A%2F%2Fec.europa.eu%2Fcefdigital%2Fwiki%2Fdownload%2Fattachments%2F78549570%2FTrends%2520report%2520on%2520electronic%2520identification_for%2520publication_v.1.1.pdf%3Fversion%3D1%26modificationDate%3D1551198712785%26api%3Dv2&usg=AOvVaw1FGeqeti2iyId_b8PUyC_M

[197] PRŮŠA J., 2015, *E-identity: Basic Building Block of e-Government*, da https://www.dnssec.cz/files/nic/doc/Jiri_Prusa_mojeID_ISTAfrica.pdf

[198] MANCA G., 24 luglio 2020, *Regolamento eIDAS, obiettivi e stato della diffusione*, da https://www.agendadigitale.eu/documenti/identita-e-firma-digitale-il-punto-sul-regolamento-eidas-obiettivi-e-stato-della-diffusione/

[199] TALARICO A., 5 febbraio 2018, *Cittadinanza digitale, che cos'è e perché è importante per i nostri diritti*, da https://www.agendadigitale.eu/cittadinanza-digitale/cittadinanza-digitale-ce-sapere-far-valere-propri-diritti/