Consiglio Nazionale del Notariato

SETTORE INFORMATICO

STUDIO N. 1-2020/DI

IL SISTEMA PUBBLICO DI IDENTITA' DIGITALE

di Giuseppe Levante

Approvato dal Settore Informatico il 07.10.2020

ABSTRACT

Il presente studio analizza le caratteristiche, il funzionamento e le prospettive del Sistema Pubblico di Identità Digitale (SPID) quale sistema di autenticazione che il Legislatore ha previsto per consentire ad imprese e cittadini di interagire con la Pubblica Amministrazione e con i privati ed ottenere dagli stessi servizi attraverso l'utilizzo di sistemi informatici quali PC o dispositivi mobili.

Nell'esaminare la natura di SPID si è tentato dapprima di fornire una definizione di servizio pubblico online e di identità digitale per poi giungere alla differenziazione tra sistemi di autenticazione, sistemi di identificazione e sistemi di sottoscrizione digitale. Questo percorso logico ha poi consentito di esaminare la normativa attualmente in vigore al fine di stabilire se fosse possibile incasellare SPID in una delle dette categorie ovvero, più verosimilmente, attestarne la natura ibrida.

Lo studio ripercorre tutta la storia di SPID, a partire dalla sua nascita, avvenuta nel 2013, in un contesto dove poche amministrazioni avevano già timidamente iniziato un percorso teso alla fruizione digitale dei servizi, ma in maniera del tutto frammentaria, fino a giungere agli ultimi provvedimenti (compreso il c.d. "D.L. Semplificazioni"), passando per un percorso di attuazione e diffusione decisamente tortuoso e difficoltoso.

SPID viene pertanto analizzato sia sotto il profilo della normativa nazionale, effettuando una analisi puntuale delle norme contenute all'interno del Codice dell'Amministrazione Digitale e dei regolamenti attuativi e linee guida che lo hanno riguardato, sia alla luce della normativa comunitaria, con particolare attenzione al Regolamento eIDAS ed alle varie Direttive e regolamenti attuativi in tema di identità digitale e procedure comuni di identificazione elettronica e di accesso ai servizi.

Inoltre, SPID viene valutato quale mezzo di comunicazione con la pubblica amministrazione idoneo a formare il c.d. "domicilio digitale", ed infine fatto oggetto di confronto con gli altri

strumenti digitali già presenti nel nostro ordinamento quali la Carta Nazionale dei Servizi (CNS), la Carta di Identità Elettronica e la firma elettronica qualificata, al fine di stabilire l'esatto perimetro di questi strumenti e valutarne affinità e differenze.

Da ultimo, si è proceduto ad effettuare una analisi delle disposizioni recate dalla nuova Direttiva (UE) 2019/1151, pubblicata nella GUCE del giorno 11 luglio 2019, in tema di "SRL online" in tema di identificazione a distanza e della idoneità di SPID a fungere da mezzo di identificazione personale di soggetti connessi da remoto, ai fini della costituzione societaria in ambito notarile.

Sommario: 1) Generalità. 2) Operatori e livelli di sicurezza. 3) Il concetto di Identità Digitale 4) Storia e percorso di attuazione. 5) Verso una gestione accentrata? 6) Le vicende inerenti al rilascio delle identità digitali. 7) SPID professionale. 8) SPID come mezzo di comunicazione per il cittadino e la Pubblica Amministrazione: il c.d. "domicilio digitale". 9) Rapporti tra SPID, Carta Nazionale dei Servizi e Carta di identità Elettronica. 10) SPID come mezzo di identificazione nella nuova "S.R.L. *online*". 11) Conclusioni.

1) Generalità.

Il complesso di attività prestate da un pubblico potere nei confronti degli utenti per il soddisfacimento di bisogni collettivi corrisponde alla definizione di servizio pubblico, il quale, in base alla Direttiva del Presidente del Consiglio dei Ministri del 27 gennaio 1994, deve ispirarsi ai principi di eguaglianza[1], imparzialità[2], continuità[3], diritto di scelta[4],

1 Nessuna distinzione nell'erogazione del servizio può essere compiuta per motivi riguardanti sesso, razza, lingua, religione ed opinioni politiche. Va garantita la parità di trattamento, a parità di condizioni del servizio prestato, sia fra le diverse aree geografiche di utenza, anche quando le stesse non siano agevolmente raggiungibili, sia fra le diverse categorie o fasce di utenti. L'eguaglianza va intesa come divieto di ogni ingiustificata discriminazione e non, invece, quale uniformità delle prestazioni sotto il profilo delle condizioni personali e sociali. In particolare, i soggetti erogatori dei servizi sono tenuti ad adottare le iniziative necessarie per adeguare le modalità di prestazione del servizio alle esigenze degli utenti portatori di handicap.

2 I soggetti erogatori hanno l'obbligo di ispirare i propri comportamenti, nei confronti degli utenti, a criteri di obiettività, giustizia ed imparzialità. In funzione di tale obbligo si interpretano le singole clausole delle condizioni generali e specifiche di erogazione del servizio e le norme regolatrici di settore.

3 L'erogazione dei servizi pubblici, nell'ambito delle modalità stabilite dalla normativa regolatrice di settore, deve essere continua, regolare e senza interruzioni. I casi di funzionamento irregolare o di interruzione del servizio devono essere espressamente regolati dalla normativa di settore. In tali casi, i soggetti erogatori devono adottare misure volte ad arrecare agli utenti il minor disagio possibile.

4 Ove sia consentito dalla legislazione vigente, l'utente ha diritto di scegliere tra i soggetti che erogano il servizio. Il diritto di scelta riguarda, in particolare, i servizi distribuiti sul territorio.

partecipazione[5], efficienza ed efficacia[6]. Con il passare degli anni si è assistito ad una sempre maggiore spinta tesa ad adeguare il servizio pubblico a continui nuovi standard tecnologici, in modo da assicurare ai cittadini un accesso diretto ai servizi offerti dalla Pubblica Amministrazione attraverso strumenti telematici. L'accesso al servizio pubblico in modalità telematica è un'esigenza molto sentita in quanto consente una maggiore fluidità ed efficacia dei traffici economici ed al tempo stesso un risparmio di costi e di tempo sia per l'utente che per l'amministrazione che offre il servizio. Queste moderne e sempre crescenti esigenze sono state cristallizzate in un gruppo di norme contenute nel Codice dell'Amministrazione Digitale[7], il quale all'art. 3 dispone che chiunque ha diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti informatici e digitali nei rapporti con la pubblica amministrazione, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo. A questo principio si aggiunge quanto stabilito dagli artt.3 *bis* e 7 del CAD in base ai quali si stabilisce che i cittadini hanno il diritto di accedere ai suddetti servizi tramite la propria identità digitale[8] in forma integrata a mezzo degli strumenti telematici messi a disposizione dalle pubbliche amministrazioni, anche attraverso dispositivi mobili.

Anche nel panorama europeo si è inteso di fatto favorire la creazione, in ambito digitale, di una base comune e condivisa per le transazioni economiche sicure fra imprese, cittadini e autorità pubbliche, così da migliorare l'efficacia dei servizi elettronici pubblici e privati, delle transazioni elettroniche e del commercio elettronico nell'Unione, al fine di eliminare le barriere esistenti all'impiego transfrontaliero dei mezzi di identificazione elettronica utilizzati negli Stati membri almeno per l'autenticazione nei servizi pubblici[9]. Questi aspetti costituiscono infatti il principale oggetto disciplinato dal Regolamento UE n.910/2014 (c.d. regolamento eIDAS)[10].

La Pubblica Amministrazione deve, pertanto, in ottemperanza alle norme sopra citate, provvedere alla riorganizzazione ed all'aggiornamento dei servizi resi, sulla base di una

5 L'utente può produrre memorie e documenti; prospettare osservazioni; formulare suggerimenti per il miglioramento del servizio. I soggetti erogatori danno immediato riscontro all'utente circa le segnalazioni e le proposte da esso formulate.

6 Il servizio pubblico deve essere erogato in modo da garantire l'efficienza e l'efficacia. I soggetti erogatori adottano le misure idonee al raggiungimento di tali obiettivi.

7 Il Codice dell'Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale, e da ultimo con il recente D.L. 16 luglio 2020 n.76, pubblicato sulla G.U.R.I n.178 del 16 luglio 2020 (c.d. "D.L. Semplificazioni"), convertito in L.11 settembre 2020 n.120.

8 L'identità digitale viene definita all'art. 1, lett. u-*quater*, del CAD come la rappresentazione informatica della corrispondenza tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale.

9 Cfr il "considerando" n.12 del Regolamento.

10 Preme segnalare come sia in corso un riesame del Regolamento, ex art.49, con lo scopo di valutare l'applicazione del quadro eIDAS anche in ambiti diversi, ponendo attenzione ai temi della identificazione elettronica, della conservazione qualificata delle firme e dei sigilli elettronici qualificati, dei servizi elettronici di recapito certificato e dei certificati qualificati di autenticazione relativi ai siti web.

preventiva analisi delle reali esigenze degli utenti e deve rendere disponibili *on-line* i propri servizi, consentendo agli utenti di esprimere una valutazione rispetto alla qualità, anche in termini di fruibilità, accessibilità e tempestività, del servizio reso[11].

Proprio per raggiungere le finalità suddette, con l'art.64, comma 2 *bis*, del CAD è stato istituito il "Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese" (SPID), il quale viene definito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, identificano gli utenti per consentire loro l'accesso ai servizi in rete. Il Sistema Pubblico di Identità Digitale (SPID), nel contesto appena delineato, rappresenta quindi la principale soluzione per assicurare a cittadini ed imprese un accesso sicuro e protetto ai servizi digitali della Pubblica Amministrazione, garantendone un elevato grado di *fruibilità* attraverso l'adozione di strumenti moderni e flessibili compresi i c.d. dispositivi *mobile*. SPID, in alternativa all'utilizzo della carta di identità elettronica (CIE) e della carta nazionale dei servizi (CNS), permette, infatti, l'identificazione informatica degli utenti attraverso la validazione dell'insieme di dati ad essi attribuiti in modo esclusivo ed univoco. Con il sistema pubblico di identità digitale si può infatti accedere ai servizi *online* con un solo *account* universalmente accettato, ed utilizzare tale autenticazione (basata su specifiche[12] diffuse ed adottate nell'ambito del progetto sperimentale *Stork*[13]) nei confronti di qualunque erogatore di servizi *online* sia italiano che dell'Unione Europea[14].

2) Operatori e livelli di sicurezza.

L'identità SPID si ottiene facendone richiesta a uno degli *identity provider* (Gestori di identità digitale) accreditati dall'Agenzia per l'Italia digitale (AgID)[15]. Il sistema SPID è infatti,

---

11 In caso di violazione degli obblighi suddetti, gli utenti, fermo restando il diritto di rivolgersi al difensore civico digitale di cui all'art. 17 del CAD, possono agire in giudizio, anche nei termini e con le modalità stabilite nel D.Lgs. 20 dicembre 2009, n.198. Inoltre, il comma 1-*quinques*, dell'art. 64 *bis* del CAD, in corso di modifica per il tramite del recente "DL Semplificazioni", dispone che La violazione dell'articolo 64, comma 3-*bis* e delle disposizioni di cui al presente articolo, costituisce mancato raggiungimento di uno specifico risultato e di un rilevante obiettivo da parte dei dirigenti responsabili delle strutture competenti e comporta la riduzione, non inferiore al 30 per cento della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei dirigenti competenti, oltre al divieto di attribuire premi o incentivi nell'ambito delle medesime strutture.

12 OASIS SAML v.2.0.

13 Un progetto condiviso su larga scala da molti paesi europei che mira a sviluppare un'infrastruttura comune per l'identità digitale, sia per le persone fisiche che per quelle giuridiche.

14 Interessante appare anche l'iniziativa denominata "Single Digital Gateway" (Sportello unico digitale europeo) che mira alla creazione di un unico punto di accesso alle informazioni sulle regole vigenti a livello nazionale ed europeo in materia di impresa, lavoro, istruzione, salute e tassazione. Il portale fornirà anche assistenza per l'accesso ai servizi più idonei alle necessità degli utenti ed entro il 2023 fornirà anche la possibilità di gestire online più di venti procedure amministrative, tra cui certificati di nascita, le dichiarazioni dei redditi e le iscrizioni all'università.

15 L'Agenzia per l'Italia digitale (abbreviato AgID) è una agenzia pubblica italiana istituita dal governo Monti. Sottoposta ai poteri di indirizzo e vigilanza del presidente del Consiglio dei ministri o del ministro da lui delegato, svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della pubblica amministrazione e al servizio dei

come già visto, un insieme aperto e federato di soggetti pubblici e privati che, previo accreditamento, gestiscono i servizi di registrazione e messa a disposizione delle credenziali di accesso e degli strumenti di accesso in rete. Pertanto, nel sistema SPID si distinguono tre tipologie di operatori:

- *Identity provider* (gestore di identità digitale): che ha il compito di fornire le credenziali di accesso al sistema (identità digitali) e gestisce i processi di autenticazione degli utenti.
- *Service provider* (fornitore di servizi): che mette a disposizione servizi digitali accessibili a coloro che sono in possesso delle identità digitali rilasciate dagli *identity provider*.
- *Attribute provider* (gestore di attributi qualificati): che fornisce attributi che qualificano gli utenti (stati, ruoli, titoli, cariche), finalizzati alla fruizione diversificata dei servizi.

L'*account* SPID è costituito da credenziali con caratteristiche differenti in base al livello di sicurezza richiesto per la tipologia di servizio di cui si intende usufruire. Il livello di sicurezza è il risultato dell'intero procedimento che sottende all'attività di autenticazione. Tale processo va dalla preliminare associazione tra un soggetto ed un'identità digitale che lo rappresenta in rete, con annessa attribuzione di credenziali in grado di comprovare tale associazione, ai meccanismi che realizzano il protocollo di autenticazione al momento della richiesta di un servizio in rete. Attualmente sono stati previsti tre livelli di sicurezza[16], ognuno dei quali corrisponde a un diverso livello di SPID:

- Il primo livello[17] permette di accedere ai servizi *online* semplicemente attraverso l'utilizzo di un nome utente e una *password* scelti dall'utente. A tale livello è associato un rischio moderato e compatibile con l'impiego di un sistema di autenticazione a singolo fattore. Questo livello può essere utilizzato nei casi in cui il danno causato da un utilizzo indebito dell'identità digitale ha un basso impatto per le attività del cittadino, dell'impresa o dell'amministrazione;
- Il secondo livello[18], necessario per servizi che richiedono un grado di sicurezza maggiore, permette l'accesso attraverso un nome utente e una password scelti dall'utente a cui però deve necessariamente aggiungersi la generazione di un codice temporaneo di accesso attraverso un dispositivo OTP (*one time password*) fisico o virtuale. A tale livello è associato un rischio notevole e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori non necessariamente basato

cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza, secondo criteri di efficienza, economicità ed efficacia.

16 I livelli di sicurezza sono stati previsti originariamente dall'art.8 del Regolamento (UE) n.910/2014, il quale distingue tra servizi che richiedono l'identificazione degli utenti con livello basso, significativo ed elevato.

17 Corrispondente al LoA2 dell'ISO-IEC 29115.

18 Corrispondente al LoA3 dell'ISO-IEC 29115.

su certificati digitali. Questo livello è adeguato per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno consistente;

- Il terzo livello[19], infine, oltre al nome utente e la *password*, richiede un supporto fisico particolare che gestisce delle chiavi crittografiche. Tale supporto può essere una *smart card* od un dispositivo per la firma digitale remota (HSM)[20]. A tale livello è associato un rischio altissimo e compatibile con l'impiego di un sistema di autenticazione informatica a due fattori basato su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti di cui all'Allegato II del Regolamento 910/2014. Questo livello è da associare a quei servizi che possono subire un serio e grave danno per cause imputabili ad abusi di identità e per tutti i servizi per i quali un indebito utilizzo dell'identità digitale può provocare un danno serio e grave.

3) Il concetto di Identità Digitale.

Con l'ottenimento di SPID all'utente viene assegnata una identità digitale cui è associato un livello di sicurezza adeguato a seconda del contesto di utilizzo. Ma cosa si intende esattamente per identità digitale?

L'identità digitale viene definita all'art. 1, lett. u-*quater*, del CAD come la rappresentazione informatica della corrispondenza (biunivoca) tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale. È intuitivo comprendere, tuttavia, che la suddetta definizione non appare sufficiente a chiarire in maniera definitiva le idee ed anzi molti potrebbero essere i dubbi ed i fraintendimenti che potrebbero scaturire da essa.

Apparentemente, infatti, il concetto di identità digitale potrebbe essere associato all'esatto corrispettivo informatico dell'identità personale. In realtà con il termine identità digitale (o ID digitale) si fa riferimento ad un concetto molto più ampio e variegato. Se infatti da un lato l'identità personale attiene essenzialmente ad un complesso di dati testuali e biometrici incorporati in un documento rilasciato da una pubblica autorità e, pertanto, si sostanzia nel complesso delle risultanze anagrafiche che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici ed a distinguerlo dagli altri consociati[21]; dall'altro il concetto di identità digitale, nella sua accezione più ampia, ricomprende tutta una serie di espressioni della personalità, che spaziano dagli *account* su *forum* o *social media* (*facebook, twitter* etc..), fino giungere a procedimenti sofisticatissimi di identificazione. Più precisamente per identità digitale s'intende sia un generico sinonimo di identità di rete (o virtuale), eventualmente anche mediante l'utilizzo di pseudonimi, sia in un'altra accezione

19 Corrispondente al LoA4 dell'ISO-IEC 29115.

20 Al momento, solo Aruba e Poste Italiane forniscono il terzo livello di sicurezza.

21 G.Renna, Identità personale ed identità digitale, in IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA, Anno XXIII Fasc.3 – 2007, Milano, Giuffrè Editore.

– prettamente tecnica – il complesso delle informazioni e delle risorse concesse da un sistema informatico (pubblico o privato) ad un utilizzatore e protette da sistemi di autenticazione che possono essere effettuate tramite password, caratteristiche biologiche (impronta digitale, vocale, riconoscimento del volto o dell'iride) od attraverso *smart card* associate ad un *id* utente[22]. All'interno del concetto di identità digitale sono, pertanto, ricompresi sia la semplice accoppiata di nome utente e password utili per l'accesso ad un sito, sia i sistemi di autenticazione più avanzati quali, ad esempio, quelli che necessitano di dispositivi OTP (come nel caso dei sistemi di *home banking*), fino a giungere addirittura ai mezzi di identificazione personale digitali quali la carta di identità elettronica, passaporto biometrico etc… .

Va comunque precisato che per quanto riguarda le identità digitali più avanzate (quali SPID, CIE etc…), il collegamento delle stesse ad una persona fisica può essere certo solo in fase di rilascio, ma non può mai esserlo in fase di utilizzo: l'ottenimento di un'identità digitale porta con sé quindi la responsabilità dell'uso personale della stessa, non affidandola ad altre persone[23].

4) Storia e percorso di attuazione.

Nel processo storico dell'informatizzazione della Pubblica Amministrazione del nostro Paese nei rapporti con cittadini ed imprese, un punto cruciale è rappresentato dal CAD (Codice Amministrazione Digitale), di cui al D.lgs. 7 marzo 2005 n.82, modificato ed integrato prima con il D.lgs. 22 agosto 2016 n.179, poi con il D.lgs. 13 dicembre 2017 n.217 e da ultimo con il recente D.L. 16 luglio 2020 n.76 (c.d. "D.L. Semplificazioni"), il quale, come già visto, ha introdotto una serie di obblighi tesi alla digitalizzazione della Pubblica Amministrazione e che in particolare all'art. 64, comma 2 *bis*, ha introdotto il concetto di sistema pubblico di identità digitale finalizzato alla fruizione da parte di cittadini ed imprese, persone fisiche e giuridiche[24], dei servizi offerti dalla Pubblica Amministrazione.

La volontà di digitalizzare, informatizzare e consentire la fruizione telematica dei servizi della Pubblica Amministrazione nasce dal desiderio di scalare la c.d. classifica DESI (*Digital Economy and Society Index*) della Commissione Europea, la quale misurava una percentuale eccessivamente bassa di accessi ai sevizi *online* dell'Italia. La classifica viene formata sulla base della diffusione della banda larga, delle competenze digitali e delle attività *online*, registrati nell'arco di un anno all'interno di un paese. Nel 2016 l'Italia si attestava al venticinquesimo posto su ventotto Paesi dell'Unione Europea[25] per digitalizzazione dell'economia e della società. In particolare, il nostro Paese era tra i c.d. "*Catching Up*": ovvero quelli con punteggio

22 Michele Nastri, L'evoluzione digitale del Notaio e la sicurezza giuridica in rete, p. 107, Amazon, 2020.
23 Michele Nastri, op. cit., p. 116.
24 Come chiarito dall'art.61, comma 2, lettera d) del D.lgs. 179/2016.
25 Al momento in cui si scrive la posizione è rimasta invariata e pertanto l'Italia risulta quartultima prima di Grecia, Bulgaria e Romania.

inferiore alla media ma il cui punteggio cresce più velocemente rispetto a quello medio della Ue nell'anno precedente[26].

Nell'ambito della digitalizzazione dei servizi della Pubblica Amministrazione, SPID non rappresenta, tuttavia, il primo esperimento. Prima della nascita del sistema SPID, invero, vi erano già stati frammentari tentativi volti alla digitalizzazione dei servizi della Pubblica Amministrazione. Infatti, enti come INPS, Agenzia delle Entrate, università e molte amministrazioni regionali e comunali, avevano predisposto autonomamente degli strumenti di attribuzione di identità digitali per la fruizione dei rispettivi servizi. La vera novità che SPID rappresentò fu, pertanto, quella di federare il sistema esistente mediante l'utilizzo di un'identità unica che potesse consentire l'accesso a tutti i servizi della Pubblica Amministrazione, ponendo fine quindi alla frammentaria esperienza precedente[27].

In tale contesto, la genesi del sistema SPID avvenne nel marzo 2013 quando il deputato Stefano Quintarelli, all'epoca Presidente del Comitato di Indirizzo dell'AgID, propose l'idea di "un *framework*[28] per autenticare l'accesso ai servizi della pubblica amministrazione" che raccolse sin da subito l'appoggio trasversale di numerosi deputati e senatori[29].

Il primo provvedimento di attuazione di SPID è rappresentato dal decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 ,recante la definizione delle caratteristiche del sistema SPID nonché dei tempi e delle modalità di adozione del sistema[30]. In particolare, l'art. 4 del DPCM ha attribuito all'AgID i compiti di: gestire l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni; curare l'aggiornamento del Registro SPID e vigilare sull'operato di tutti i soggetti che partecipano al sistema; stipulare apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità. Inoltre, il DPCM agli artt. 1 e 13 stabilisce la disciplina di accesso dei fornitori, pubblici e privati, di servizi al sistema SPID a mezzo di apposita convenzione, prevedendo espressamente l'obbligo di non discriminare gli utenti sulla base del gestore di identità digitale prescelto dai medesimi. Infine, all'art. 15 vengono stabilite specifiche norme per l'adesione allo SPID da parte dei fornitori privati di servizi, per i quali la convenzione relativa potrà regolare in particolare anche i corrispettivi che gli stessi dovranno ai gestori dell'identità digitale ed ai gestori di attributi qualificati per i servizi di autenticazione.

---

26 Il gruppo di Paesi che non registra questa velocità di crescita viene chiamato "*Falling Behind*".

27 Come si legge nella relazione illustrativa al Decreto, questo sistema "permetterà di superare la complessità della situazione attuale per cui ogni pubblica amministrazione o ente pubblico che garantisce servizi *on-line* richiede proprie modalità di registrazione e di utilizzo dei servizi".

28 Cioè una struttura – quadro con regole uniformi.

29 Il nucleo bipartisan prese il nome di "Intergruppo innovazione". Gli intergruppi sono transcamerali (con componenti sia tra i deputati sia tra i senatori) e transpartitici. Nascono per portare avanti tematiche ed iniziative bipartisan.

30 Il DPCM stabilisce le caratteristiche di SPID, permettendo agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati onde consentire ai fornitori di servizi l'immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano.

Successivamente, con la Determinazione n. 44 del 28 luglio 2015 e n.189 del 22 luglio 2016, sono stati emanati, ed in seguito parzialmente modificati, da AgID i quattro regolamenti[31], previsti dall'articolo 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014, attraverso i quali il sistema SPID è divenuto operativo. In particolare, in base all'art.3 del Regolamento recante le modalità attuative per la realizzazione dello SPID, AgID ha predisposto lo schema di convenzione per consentire ai gestori di presentare domanda per ottenere l'iscrizione nel relativo registro.

Tra il 19 dicembre 2015 e il 12 maggio 2017, nel rispetto delle procedure previste dalle norme, l'AgID ha accreditato i primi sette gestori di Identità SPID[32] e dal 15 marzo 2016 i primi tre gestori di identità digitale hanno incominciato a rilasciare le prime identità SPID a cittadini e imprese richiedenti. Fu prevista inizialmente l'adesione a SPID di quindici amministrazioni pilota[33].

Dopo dieci mesi dal debutto di SPID, il Governo dichiarò di aver raggiunto quota un milione di erogazioni di identità digitali. Tuttavia, nonostante la partenza decisa, la diffusione successiva subì numerosi rallentamenti. Ciò avvenne in quanto l'accelerazione iniziale fu essenzialmente dovuta ad iniziative tendenzialmente "*one shot*" e quindi irripetibili: come ad es. quella agganciata al c.d. "*Bonus Docenti"* previsto dalla legge 13 luglio 2015, n.107; od ancora quella relativa al c.d. "*Bonus Cultura*" riservato ai maggiorenni dell'anno 2016. Una volta esaurite le suddette iniziative, la diffusione delle identità digitali è risultata tutta in salita[34].

Le appena cennate difficoltà furono dovute anche alla gracile sostenibilità economica del Sistema, così come congegnato. Il sistema federato pubblico-privato, innovativo sulla carta, era portatore in realtà di un insanabile conflitto concettuale. Se da un lato si poneva il generale interesse da parte dello Stato a che le identità digitali fossero erogate gratuitamente ai cittadini, dall'altro si contrapponevano le ovvie logiche di impresa di cui sono portatori i gestori privati. E' chiaro che l'erogazione delle identità digitali, alla quale sono connesse le necessarie e complesse operazioni di identificazione dell'utente (e conseguenti responsabilità), corrisponde ad un costo da sostenere per l'erogatore privato, il quale ha l'ovvio interesse a recuperarlo se non, magari, a trasformarlo in utile. Inoltre, la scarsa diffusione di SPID, da un lato ha reso restie le amministrazioni a fornire nuovi servizi e dall'altro

31 Il regolamento recante le modalità attuative per la realizzazione dello SPID; il regolamento recante le regole tecniche; il regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale; il regolamento recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale.

32 Infocert S.p.A., Poste Italiane S.p.A. e Tim (attraverso la società Trust Technologies del gruppo Telecom Italia), Aruba PEC S.p.A., Sielte S.p.A., Namirial S.p.A e Register.it S.p.A. .

33 Agenzia delle entrate, Equitalia, INPS, INAIL, Comune di Firenze, Comune di Venezia, Comune di Lecce, Comune di Genova, Regione Toscana, Regione Liguria, Regione Emilia-Romagna, Regione Friuli-Venezia Giulia, Regione Lazio, Regione Piemonte e Regione Umbria.

34 Nel 2019, in base ai dati ufficiali, erano 3.593 le pubbliche amministrazioni abilitate al sistema SPID, eroganti complessivamente 3.963 servizi *online*. Nel primo semestre del 2020, soprattutto a causa della pandemia scatenata dal virus da Sars-Cov-2 e della maggiore ed improvvisa diffusione dei procedimenti digitali conseguente alle restrizioni della libertà di circolazione dei cittadini, il tasso medio di crescita settimanale delle identità erogate è risultato raddoppiato, ed il numero complessivo di erogazioni ha superato quota 7 milioni.

ha fatto pervenire sempre meno richieste di rilascio di identità nei confronti degli operatori. Per tentare di assicurare una sostenibilità economica al Sistema si iniziò a pensare, quindi, di implementare alcune funzioni avanzate prevedendo costi per gli utenti interessati alle stesse. La più evidente applicazione pratica di questo tentativo fu rappresentato dal c.d. SPID professionale, di cui si parlerà più avanti.

In seguito alla pubblicazione sulla Gazzetta Ufficiale europea del 10 settembre 2018, successivamente integrata nella Gazzetta del successivo 26 settembre n.344/11, è stata resa nota la comunicazione mediante la quale SPID è stato notificato quale sistema di autenticazione nazionale conforme al Regolamento eIDAS, con l'indicazione dei tre livelli oggetto di notifica (elevato, significativo e basso) corrispondenti ai tre livelli di accesso a SPID. Ciò ha consentito ai cittadini italiani di poter accedere ai servizi che gli altri paesi membri hanno dovuto rendere accessibili *online* entro il mese di settembre del 2019.

5) (segue) Verso una gestione accentrata?

Sulla base della normativa richiamata precedentemente, SPID veniva delineato sulla base di un modello federale e misto, pubblico-privato: da un lato vi erano le amministrazioni deputate a fornire servizi; dall'altro i privati accreditati con il compito di rilasciare le identità digitali utili ad usufruire dei servizi forniti dalle prime. In realtà, da un punto di vista meramente legislativo, alla Pubblica Amministrazione non era affatto preclusa la possibilità di rilasciare identità digitali, ma per una volontà politica più o meno espressa si spinse affinché questo tipo di attività venisse svolta esclusivamente dai privati.

La scarsa diffusione di SPID ed il crescente disinteresse dimostrato dai gestori privati (derivante come detto dalla diseconomicità del sistema stesso) ha fatto sì che lo Stato iniziasse a riflettere circa la possibilità di accentrare la gestione delle identità. Ed è proprio quello che stava per accadere con l'emendamento 42.24 al decreto legge 30 dicembre 2019 n.162, presentato dal Governo, e successivamente ritirato, con il quale si proponeva di modificare pesantemente la normativa vigente. L'emendamento tentava di intervenire nella materia dell'attuazione dell'agenda digitale e della trasformazione digitale del Paese, già oggetto dell'art. 42 del citato decreto legge, implementando le modifiche al Codice dell'Amministrazione Digitale. In sintesi, l'emendamento in parola prevedeva che lo Stato diventasse *Identity Provider* unico quale soggetto deputato all'erogazione ed alla gestione dell'identità medesima, nonché al relativo sistema di funzionamento. Prevedeva, inoltre, che le convenzioni già firmate con i gestori privati fossero portate a scadenza, nonché la definitiva abrogazione del sistema SPID prevedendo un sistema di conversione delle identità già rilasciate e la sua sostituzione con l'identità digitale abbinata al rilascio della carta di identità elettronica (CIE), per i servizi che richiedono l'identificazione degli utenti con livelli basso, significativo ed elevato, oppure attraverso credenziali di accesso a uno o

più fattori per i servizi che richiedono l'identificazione degli utenti con livelli basso e significativo[35].

In un certo senso, sembra andare nella medesima direzione centripeta anche l'emanazione, avvenuta il 21 novembre 2019[36], delle linee guida per la realizzazione di un modello di RAO[37] pubblico. Le regole tecniche, redatte secondo la procedura fissata dall'art. 71 del CAD prevedono, appunto, un modello di RAO pubblico, intendendo per esso la Pubblica Amministrazione che svolge l'attività di verifica dell'identità personale dei cittadini, al fine del rilascio dell'identità digitale SPID. Obiettivo delle Linee Guida è quello di permettere alle PA di effettuare l'identificazione delle persone fisiche, attività, questa, propedeutica al rilascio dell'identità digitale SPID da parte degli *Identity Provider* accreditati. Pertanto, le pubbliche amministrazioni che intendano riconoscere le persone fisiche, ai fini del rilascio dell'Identità digitale, e quindi che siano interessate ad essere riconosciute come RAO pubblico sono tenute a fare richiesta all'Agid. L'Agenzia informerà gli *identity provider* in merito ai soggetti che avranno richiesto il riconoscimento suddetto, mentre gli *identity provider*, a loro volta, informeranno l'Agenzia ogni qualvolta intendano utilizzare le procedure di identificazione effettuate dai RAO pubblici. L'agenzia metterà, in tal modo, nella disponibilità di entrambi i soggetti il certificato di sigillo elettronico che consente la comunicazione sicura tra i predetti soggetti per il rilascio del *token* personale agli utenti.

6) Le vicende inerenti al rilascio delle identità digitali.

Come già visto, attualmente gli *Identity Provider* sono rappresentati da soggetti privati che hanno il compito di rilasciare l'identità digitale nei confronti dei cittadini che ne facciano richiesta. Sono abilitati al rilascio delle identità digitali solo i gestori iscritti nell'apposito registro gestito da AgID, accessibile telematicamente. Per rivestire il ruolo di *Identity Provider* è necessario rispettare alcuni requisiti previsti dall'art.10, comma 3, lett. A) del DPCM del 24 ottobre 2014 e dall'art. 1 del Regolamento recante le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale[38].

---

35 Nel sistema delineato avrebbe preso parte l'Istituto Poligrafico e Zecca dello Stato S.p.A. (che si sarebbe dovuto occupare della realizzazione e dell'esercizio del sistema di funzionamento dell'identità digitale) e la società PagoPA (che avrebbe dovuto fornire servizi informatici per lo sviluppo e l'implementazione del sistema all'Istituto Poligrafico su base convenzionale). L'emendamento mirava, quindi, a creare un sistema di identità digitale gratuito, costruito essenzialmente sul modello della già prevista Carta d'Identità Elettronica (C.I.E.) che, nel prospettato nuovo sistema, sarebbe risultata arricchita sotto il profilo tecnologico, con modalità d'uso più moderne e sicure.

36 Pubblicate sulla GURI del giorno 1 febbraio 2020.

37 *Registration Authority Office*

38 Più in particolare, tale norma originariamente prevedeva, solo per i soggetti privati, la sussistenza obbligatoria di un capitale sociale pari ad almeno cinque milioni di euro. Di fronte a tale previsione, alcune associazioni di rappresentanza dei *providers* ponevano la questione innanzi al TAR Lazio per l'irragionevolezza del suddetto requisito minimo che appariva come sproporzionato e non giustificato da ragioni tecniche, con effetti di chiusura del mercato. Il TAR Lazio, pertanto, accogliendo l'istanza, con sua sentenza n.9951/2015, annullava l'art.10, comma 3, lett. a) del DPCM del 24 ottobre 2014, qualificando tale previsione come un ingiustificato sbarramento

Ciò premesso, appare chiaro come il rilascio delle identità digitali dai soggetti a ciò abilitati, rappresenta un fondamentale tassello del funzionamento del sistema SPID. L'identità digitale, infatti, come già visto, può essere definita come la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale. Essa, quindi, per essere rilasciata, necessita della c.d. registrazione e cioè nell'insieme delle procedure informatiche, organizzative e logistiche mediante le quali, con adeguati criteri di gestione e protezione, viene attribuita un'identità digitale ad un utente, previa raccolta, verifica e certificazione degli attributi da parte del gestore dell'identità digitale a un utente, garantendo l'assegnazione e la consegna delle credenziali di accesso prescelte in modalità sicura.

Piu precisamente, l'adesione e l'iscrizione al sistema SPID si compone di una serie di processi, connessi tra loro, che prendono avvio dalla richiesta di una identità digitale da parte dell'utente; proseguono con la dimostrazione, l'esame e la verifica dell'identità e si concludono con il rilascio delle credenziali SPID e la successiva conservazione e registrazione dei documenti. È utile ricordare come, ai sensi dell'art.2 del Regolamento recante le modalità attuative per la realizzazione dello SPID, il Sistema deve conformarsi al principio di necessità del trattamento dei dati di cui all'art. 3 del D.Lgs. 30 giugno 2003 n.196, in base al quale i sistemi informativi ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi[39].

La compilazione del modulo di adesione costituisce la prima attività da cui parte il processo di richiesta di una nuova identità digitale SPID. Il modulo contiene le informazioni necessarie e sufficienti per l'identificazione del richiedente. Tali informazioni sono sostanzialmente di due tipologie, e cioè: *(i)* gli attributi identificativi, consistenti nei dati relativi all'identità del richiedente, e *(ii)* gli attributi secondari che consentono di gestire in maniera efficace il rapporto tra il gestore delle identità digitali ed il sottoscrittore. Per le persone fisiche sono obbligatorie le informazioni relative a cognome e nome, sesso, data e

---

per l'accesso al mercato nonché in contrasto con i principi comunitari di tutela della concorrenza, parità di trattamento e non discriminazione, che si pongono quali diretti parametri di legittimità dell'atto nazionale. Chiamato a pronunciarsi sul merito, il Consiglio di Stato con sua decisione n.1214/2016 confermava la appena richiamata sentenza annullando definitivamente il requisito di capitale sociale minimo. A seguito delle appena sopracitate pronunce però non era stato interrotto il processo di applicazione del regolamento n.44/2015 dell'AgID, il quale proprio in virtù di quanto previsto dal DPCM 24 ottobre 2014 disciplinava i requisiti per la gestione ed accreditamento per i gestori di identità digitale prevedendo nuovamente il requisito minimo di capitale. Le medesime ricorrenti, pertanto, decidevano di impugnare il suddetto regolamento (art. 1, comma 6) rilevando che il requisito minimo di capitale sociale ivi previsto non era ricavabile da alcuna fonte normativa di grado superiore all'art.10, comma 3, DPCM 24 ottobre 2014, poi annullato dal TAR Lazio con sentenza 9951/2015 e confermata dal Consiglio di Stato con sua decisione n.1214/2006. Su questo punto il tribunale amministrativo si è pronunciato a sostegno delle ricorrenti dichiarando che la previsione di tale requisito risultava illegittima in virtù dell'annullamento in via giurisdizionale della norma contenuta nel DPCM 24 ottobre 2014. Il Tribunale Amministrativo ha altresì accolto la censura relativa alla previsione di polizze assicurative di importo molto elevato se rapportato al numero di identità digitali gestite, salvo il caso in cui i rischi per lo svolgimento dell'attività di gestione delle identità digitali siano tali da poter arrecare possibili danni a terzi.

39 I trattamenti dei dati personali in applicazione del detto Regolamento sono effettuati esclusivamente per le finalità previste dall'art. 64 del CAD e dall'art. 2, comma 2, del DPCM 24 ottobre 2014.

luogo di nascita, codice fiscale, indirizzo di residenza ed estremi del documento di riconoscimento presentato per l'identificazione. Per le persone giuridiche, invece, oltre ai dati dell'ente (denominazione e/o ragione sociale, codice fiscale o partita iva, indirizzo della sede legale) è necessaria l'identificazione della persona fisica individuata attraverso una certificazione con indicazione degli amministratori e/o dei rappresentanti legali ovvero, in alternativa, attraverso una procura notarile[40].

Sia per le persone fisiche che per le persone giuridiche è necessario indicare gli attributi secondari, e cioè almeno un indirizzo di posta elettronica[41] ed un recapito di telefonia mobile. Entrambi dovranno essere certificati dal gestore di identità digitale ad esempio inviando una mail all'indirizzo di posta elettronica dichiarato contenente un link ad un indirizzo di verifica e certificazione, oppure inviando un SMS al numero di cellulare con un codice numerico di controllo che deve essere riportato nel SMS di risposta[42].

Di particolare rilevanza è il processo di dimostrazione dell'identità consistente nell'acquisizione e accertamento di informazioni sufficienti ad identificare un'entità per uno specifico livello di sicurezza di autenticazione informatica in ambito SPID. L'identificazione può avvenire tramite esibizione a vista ed acquisizione del modulo di adesione firmato presentando un valido documento d'identità se il soggetto richiedente è persona fisica, una certificazione od una procura notarile attestante i poteri di rappresentanza se il richiedente è una persona giuridica.

Ai sensi dell'art. 8 del Regolamento recante le modalità attuative, è ammessa l'identificazione della persona fisica in modalità remota: in questo caso sono necessari, da parte del richiedente, il possesso in un PC collegato in rete, una *webcam* ad esso collegata ed un sistema audio funzionante. Altra modalità di autenticazione è quella informatica, prevista dall'art. 11 del citato Regolamento, che si realizza compilando, e sottoscrivendo elettronicamente, i moduli di adesione informatici posti a disposizione in rete dal gestore

---

40 Come avviene anche per il rilascio delle firme digitali, il sistema SPID prevede che l'*account* sia assegnato ad una persona fisica che assume la veste di rappresentante legale. Il regolamento eIDAS, artt. 35 e seguenti, seppur per altre finalità, prevede uno strumento diverso, corrispondente ad un sigillo elettronico, che può essere direttamente associato alla persona giuridica. Il sigillo elettronico può definirsi come una tecnica di identificazione della persona giuridica, adeguato a svolgere funzioni probatorie ma a differenza del dispositivo di firma digitale è utile solo a garantire l'origine e l'integrità dei dati, non ad apporre una sottoscrizione ad un documento.

41 Sotto tale profilo il Garante della Privacy, in conformità all'art.36 del GDPR, con provvedimento n.207 del 14 novembre 2019, si è pronunciato in maniera critica proprio in riferimento all'acquisizione dell'indirizzo *e-mail*, giacché, come disposto ai sensi dello schema di decreto, "verrebbe utilizzato anche con finalità di contatto con il beneficiario per comunicazioni attinenti all'attribuzione e all'utilizzo della Carta Elettronica". Pertanto, tutti i dati inerenti ai soggetti beneficiari, per i fini di utilizzo della Carta Elettronica, acquisiti tramite SPID, ivi includendo l'indirizzo *e-mail*, sono gestiti e trattati da SOGEI, società che opera in nome e per conto del Ministero. Nel caso di specie, SOGEI andrebbe a raccogliere i dati di autenticazione ad ogni accesso al servizio, memorizzando gli stessi nel registro delle transazioni, in qualità appunto di *service provider*. Sul punto, quindi, il Garante ha osservato che, posto che SPID consente di identificare in maniera univoca l'identità di determinati soggetti nei confronti dei fornitori dei servizi, sarebbe opportuno percorrere una via alternativa alla memorizzazione dell'indirizzo *e-mail,* offrendo invece ai beneficiari la possibilità di modificare il proprio indirizzo *e-mail* per la ricezione delle comunicazioni.

42 Alessandro Mastromatteo e Benedetto Santacroce in *Fisco, 2015, 13, 1244*.

dell'identità digitale. Inoltre, ai sensi dell'art. 9 del suddetto Regolamento, il richiedente che già possieda documenti digitali di identità, come ad esempio la tessera sanitaria *TS-CNS*, la *CNS* (Carta Nazionale dei Servizi) o carte ad essa conformi, può essere validamente riconosciuto tramite di essi[43][44].

Identificato il richiedente occorre procedere, a cura del gestore delle identità, al controllo delle informazioni confrontando i dati forniti con informazioni precedentemente convalidate ed il legame con il soggetto richiedente. La verifica dell'identità differisce infatti dalla sua dimostrazione: è necessaria la convalida delle informazioni di identità attraverso sorgenti addizionali – fonti autoritative, in particolare utilizzando convenzioni stipulate con AgID o, se non sufficienti, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti.

L'identità digitale SPID è composta, come detto, da un identificativo e da credenziali. E' possibile avere, in teoria, più di una identità digitale SPID, anche con diversi livelli di sicurezza, con l'opportunità di rivolgersi a differenti gestori di identità digitale. Tuttavia, l'identificativo deve essere univoco all'interno del dominio di ciascun gestore. Il Gestore deve in particolare definire, nell'ambito del proprio dominio, un "*account-ID*" univoco composto dall'indirizzo di posta elettronica dichiarato dal titolare dell'identità digitale.

L'identità digitale, successivamente al rilascio, può essere revocata, e cioè disattivata definitivamente ovvero sospesa temporaneamente. Ai sensi, infatti, dell'art. 8, comma 3 e art. 9 del DPCM 24 ottobre 2014, il gestore dell'identità digitale revoca l'identità digitale: se la stessa risulta non attiva per un periodo superiore a ventiquattro mesi; per decesso della persona fisica o per estinzione della persona giuridica; e, infine, per uso illecito dell'identità digitale. La revoca è il processo che annulla permanentemente la validità delle credenziali. Diversamente la sospensione è associata ad un processo di annullamento temporaneo.

7) SPID professionale.

Come si è già avuto modo di vedere in precedenza, al fine di tentare di rendere il Sistema economicamente sostenibile si è intrapresa la strada delle c.d. identità "*avanzate*" e cioè di particolari identità il cui rilascio giustificasse un determinato costo a carico del richiedente. Sotto tale aspetto il primo tentativo è rappresentato dal c.d. "SPID professionale", ovvero di quella tipologia di identità digitale utile a provare l'appartenenza

43 L'identificazione a distanza è anche ammessa in tema di antiriciclaggio dall'art. 19, comma 1, lett. a), D.Lgs. 231/2007, e viene utilizzata anche al procedimento di rilascio delle firme elettroniche qualificate da parte dei gestori. I certificatori che hanno reso effettivamente disponibile questa possibilità sono solamente Namiral ed Infocert.

44 Invero, la procedura di identificazione da remoto, non era affatto imposta né dal regolamento eIDAS, né dal Regolamento esecutivo UE n.2015/1502 della Commissione Europea dell'8 settembre 2015, il cui allegato agli articoli 2.1.2 e 2.1.3 disciplina le modalità con cui effettuare il controllo e la verifica dell'identità delle persone fisiche e giuridiche che richiedono uno strumento di identificazione elettronica.

di una persona fisica all'organizzazione di una persona giuridica e/o la sua qualità di professionista, secondo la definizione fornita dalle "Linee Guida per il rilascio delle identità digitali per uso professionale", di cui alla determinazione n.318 del 5 novembre 2019[45].

Precedentemente all'emanazione delle Linee Guida, SPID poteva già essere usato dai professionisti per accedere ai servizi *online* degli enti pubblici, ma l'accesso avveniva da "semplici" cittadini. Grazie alle suddette "Linee Guida" è stata attivata, invece, una nuova funzionalità, attesa da numerose pubbliche amministrazioni e da privati, che consentirà l'apertura di nuovi servizi *online*, superando gli ostacoli all'uso della propria identità digitale per scopi lavorativi.

Il nuovo SPID per uso professionale permetterà, quindi, di farsi riconoscere da una pubblica amministrazione, o da un ente privato, in quanto professionista od appartenente ad una organizzazione, e consentirà di accedere ad alcuni servizi all'uopo riservati[46]. Precisa, tuttavia, l'art.1 delle "Linee Guida" che le identità in questione, al contrario, non costituiscono prova dei poteri di rappresentanza di una persona giuridica dei quali una persona fisica è eventualmente in possesso né l'appartenenza di un professionista ad un determinato ordine professionale o altro elenco qualificato. Abbinato all'identità professionale risulterà pertanto solamente un codice che qualifica, in maniera generica, il titolare come professionista, senza ulteriori dettagli[47].

Con la pubblicazione delle suddette "Linee guida" si è pertanto tracciata la disciplina dell'erogazione delle identità digitali professionali stabilendo il ruolo degli *identity provider* e delle organizzazioni, la forma ed il contenuto degli accordi tra i primi e questi ultimi nonché i limiti e gli obblighi scaturenti dalla delega rilasciata all'organizzazione per la gestione delle credenziali dei propri dipendenti e/o rappresentanti. Proprio con riguardo all'ultimo aspetto trattato, il gestore dell'identità digitale può demandare ad una organizzazione la verifica dell'identità dei soggetti cui fornire l'identità digitale per uso professionale. L'organizzazione è tecnicamente la persona giuridica che stipula un accordo con il gestore dell'identità digitale SPID al fine del rilascio delle identità digitali in favore dei soggetti che agiscono in qualità di dipendenti o, comunque, in nome o per conto dell'organizzazione stessa. Prima di sottoscrivere l'atto che regola il rapporto tra le parti,

45 Come già detto, il Regolamento eIDAS, artt. 35 e seguenti, seppur per altre finalità, prevede uno strumento diverso, corrispondente ad un sigillo elettronico, che può essere direttamente associato alla persona giuridica. Il sigillo elettronico può definirsi come una tecnica di identificazione della persona giuridica, adeguato a svolgere funzioni probatorie ma a differenza del dispositivo di firma digitale è utile solo a garantire l'origine e l'integrità dei dati, non ad apporre una sottoscrizione ad un documento. Sempre il Regolamento eIDAS agli artt. 24 e 28 prevede la possibilità che al certificato di firma qualificata possa essere eventualmente associato un attributo aggiuntivo specifico della persona fisica o giuridica. All'interno del CAD, invece, il riferimento ad attributi qualificati è contenuto all'art. 6 *bis*, comma 2 *bis* (a proposito degli ordini professionali e degli elenchi INI-PEC) e all'art. 64, comma 2 *decies* (con riferimento al diritto delle pubbliche amministrazioni di usufruire gratuitamente delle verifiche rese disponibili dai gestori di attributi qualificati).

46 Si pensi, ad esempio, ai servizi erogati dall'INPS e dall'Agenzia delle Entrate riservati ai consulenti del lavoro ed ai commercialisti.

47 L'identità digitale per uso professionale conterrà l'attributo-estensione "*Purpose"*, valorizzato con codice **P**.

l'*identity provider* deve verificare la reale esistenza del soggetto giuridico che costituisce parte del rapporto[48].

Dalle linee guida (art.6) può, inoltre, ricavarsi la distinzione tra utenza di governo e utenza di gestione: la prima è utilizzabile per l'accesso al sistema al fine di gestire le identità professionali (visualizzare l'elenco, richiedere la revoca etc.); la seconda è utile soprattutto al fine di inserire i dati identificativi dei soggetti eleggibili ad ottenere l'identità digitale professionale oltre che a dichiarare di aver ottemperato alla verifica dell'identità del soggetto richiedente.

Al momento in cui si scrive i gestori di identità digitali che forniscono *ID* per uso professionale sono solamente due[49].

8) SPID come mezzo di comunicazione per il cittadino e la Pubblica Amministrazione: il c.d. "domicilio digitale".

Ad oggi il sistema SPID è facoltativo ed il suo utilizzo è rimesso alla scelta del cittadino. Tuttavia, non è inverosimile immaginare che un futuro provvedimento possa stabilire il momento a partire dal quale tutte le comunicazioni tra gli uffici pubblici e i cittadini debbano necessariamente avvenire *online* attraverso un domicilio digitale. Ed anzi già l'art. 3-*bis*, comma 3 *bis* del CAD dispone che con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per la semplificazione e la pubblica amministrazione, sentiti l'AgID e il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, è stabilita la data a decorrere dalla quale le comunicazioni tra i soggetti di cui all'articolo 2, comma 2[50], e coloro che non hanno provveduto a eleggere un domicilio digitale ai sensi del comma 1-*bis*, avvengono esclusivamente in forma elettronica. Inoltre, il nuovo "D.L. Semplificazioni"[51] modificando il secondo periodo del citato art. 3-*bis*, comma 3 *bis*, ha stabilito che con lo stesso decreto sono determinate le modalità con le quali ai predetti soggetti può essere reso disponibile un domicilio digitale ovvero altre modalità con le quali, anche per superare il divario digitale, i documenti possono essere messi a disposizione e consegnati a coloro che non hanno accesso ad un domicilio digitale.

---

48 L'art. 8 delle Linee Guida disciplina anche il contenuto minimo che l'accordo deve avere, prevedendo che lo stesso deve contenere: i nominativi dei soggetti dell'organizzazione che hanno il potere di autorizzare il rilascio e la revoca delle credenziali; un indirizzo di posta elettronica certificata dell'organizzazione; il nominativo ed i recapiti dei rispettivi responsabili del rapporto.

49 Namiral e Register, quest'ultima limitatamente alle persone fisiche.

50 E cioè: a) pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione; b) gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse; c) società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b).

51 D.L. 16 luglio 2020 n.76, pubblicato sulla G.U.R.I. n.178 del 16 luglio 2020.

Per attivare il domicilio digitale non è sufficiente un *account* SPID ma è necessario disporre anche di un indirizzo di posta elettronica certificata abbinato al primo a seguito di conforme dichiarazione dell'utente. Una volta dichiarato l'indirizzo PEC, esso potrà essere utilizzato dalle pubbliche amministrazioni soggette al CAD per tutte le comunicazioni e notifiche al cittadino.

Ai sensi dell'art.6 del CAD, le comunicazioni elettroniche trasmesse al domicilio digitale producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta, salvo che la legge disponga diversamente. Le suddette comunicazioni si intendono spedite dal mittente se inviate al proprio gestore e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo.

Ai sensi degli artt. 6 *bis*, *ter* e *quater* del CAD, sono stati istituiti gli indici dei domicili digitali, per imprese e professionisti, pubbliche amministrazioni e cittadini, che, come tutti gli Indici nazionali, sono destinati in futuro a confluire nell'Anagrafe della popolazione residente (ANPR). La consultazione on-line degli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater* è consentita a chiunque senza necessità di autenticazione e gli elenchi sono realizzati in formato aperto. In assenza di preventiva autorizzazione del titolare dell'indirizzo, è vietato l'utilizzo dei domicili digitali per finalità diverse dall'invio di comunicazioni aventi valore legale o comunque connesse al conseguimento di finalità istituzionali.

9) Rapporti tra SPID, Carta Nazionale dei Servizi, Carta di identità Elettronica e firma elettronica.

Nel panorama dell'informatizzazione dei processi burocratici in Italia, il sistema SPID viene in realtà affiancato da altre tipologie di identità digitali, la cui coesistenza può ingenerare ovvi motivi di confusione. Di tali aspetti si è già, in parte, accennato nel primo paragrafo.

Una importante tipologia di identità digitale è rappresentata dalla Carta Nazionale dei Servizi (CNS), la quale è un documento personale che si affianca alla Carta di Identità Elettronica (CIE). La CNS ha l'obiettivo di consentire la fruizione dei servizi previsti per la CIE agli utenti che non dispongono ancora del nuovo documento elettronico e, da qualche tempo, integra le funzioni della tessera sanitaria del Servizio Sanitario Nazionale (TS-CNS). La diffusione della CNS viene disciplinata dal Regolamento di cui al DPR 2 marzo 2004 n.117, emanato a norma dell'art.27, comma 8 lettera b), della Legge 16 gennaio 2003, n.3.

La già citata Carta di Identità Elettronica[52] è, invece, un documento di riconoscimento che ha sostituito la carta di identità in formato cartaceo[53]. Al pari della sua versione analogica, la CIE attesta l'identità del cittadino ed è inoltre valida come documento per l'espatrio. Essa è anche utile per identificarsi ed usufruire di servizi per i quali è richiesto un documento di riconoscimento ed a seguito della modifica portata dal c.d. "Decreto Semplificazioni" all'art.64 del CAD, l'accesso a tutti i servizi in rete erogati dalle pubbliche amministrazioni dovrà essere consentito tanto tramite SPID, quanto tramite CIE. La CIE può essere utilizzata anche per richiedere un'identità digitale SPID, sia relativamente alla procedura che prevede l'identificazione di presenza sia in modalità remota. La sua introduzione è volta ad incrementare i livelli di certezza mediante l'adeguamento delle caratteristiche del supporto agli standard internazionali di sicurezza ed a quelli anticlonazione e anticontraffazione in materia di documenti elettronici.

Vale la pena, adesso, soffermarsi circa la differenza che intercorre tra sistemi di autenticazione e sistemi di identificazione (o riconoscimento) personale. Come visto nel primo paragrafo, sia i sistemi di autenticazione che quelli di riconoscimento personale elettronici appartengono alla ben più ampia categoria delle identità digitali. Tuttavia, il concetto di autenticazione informatica, a ben vedere, attiene a quel processo teso a validare l'accesso di un utente all'interno di un determinato sistema informatico sulla base dell'inserimento, da parte del soggetto stesso, di credenziali (normalmente nome utente e password). La digitazione delle credenziali al contempo consente al sistema di riconoscere l'identità del soggetto che le immette, ma a detto riconoscimento deve attribuirsi una valenza essenzialmente privatistica.

Il concetto di riconoscimento personale va, invece, inquadrato in chiave prettamente pubblicistica. Proprio sotto tale aspetto può essere utile elencare alcune caratteristiche comuni a tutti i mezzi di riconoscimento personali quali: la presenza di un dato biometrico[54] incorporato nel medesimo documento identificativo; la competenza esclusiva al rilascio in

52 Già prevista dalle leggi Bassanini nel 1997, ebbe la sua genesi effettiva nel 2001 con l'emissione in ottantatré Comuni di un primo modello sperimentale (v.1.0). Nel 2004 venne introdotta una seconda versione sperimentale (v.2.0) per giungere poi, a partire dal 1 gennaio 2006, ad una versione pronta per l'ampia diffusione (v.3.0).

53 La CIE ha le dimensioni di un bancomat ed è costituita: da un supporto di materiale plastico in policarbonato, su cui sono stampati a laser la foto e i dati del cittadino, protetti con elementi e tecniche di anticontraffazione, come ologrammi e inchiostri speciali; un microchip contactless che contiene: i sati personali, la foto e le impronte del titolare; le informazioni per consentire l'autenticazione in rete da parte del cittadino ai servizi erogati in rete da pubbliche amministrazioni ed imprese; ulteriori dati per la fruizione di servizi a valore aggiunto.

54 L'art. 4, par. 1, n. 14, del GDPR, definisce i dati biometrici "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici". L'art. 35, comma secondo, del DPR 28 dicembre 2000, n.445, dispone che "sono equipollenti alla carta di identità il passaporto, la patente di guida, la patente nautica, il libretto di pensione, il patentino di abilitazione alla conduzione di impianti termici, il porto d'armi, le tessere di riconoscimento, purché munite di fotografia e di timbro o di altra segnatura equivalente, rilasciate da un'amministrazione dello Stato". Al contempo il regolamento UE 2019/1157 all'art.3, comma quinto, stabilisce la tipologia di dati biometrici che devono essere necessariamente presenti nel documento di riconoscimento digitale.

capo allo Stato[55]; la obbligatorietà, nella misura in cui non può esservi cittadino dello Stato (minorenne o maggiorenne che sia) che possa privarsene.

Relativamente al tema che qui ci interessa, occorre precisare che, sebbene SPID difetti dei suddetti requisiti tipici dei mezzi di riconoscimento personale, recenti modifiche normative hanno sostanzialmente parificato quest'ultimo alla CIE, quanto meno nell'ambito del riconoscimento del soggetto da remoto nelle transazioni elettroniche e per l'accesso ai servizi.

Un primo esempio è rappresentato dalle recenti modifiche alla normativa antiriciclaggio la quale all'art. 19 del D.Lgs. 16 novembre 2007, n.231, prevede che l'obbligo di identificazione si consideri assolto anche senza la presenza della persona fisica del cliente qualora questi sia in possesso di un'identità digitale di livello almeno significativo, nell'ambito del sistema dell'art. 64 del CAD (quindi SPID), nonché di un certificato per la generazione di firma digitale rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione Europea a norma dell'art. 9 del Regolamento UE n.910/2014 o identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'AgID.

Inoltre, sempre il recente "DL Semplificazioni" ha aggiunto, tra l'altro, all'art. 64 del CAD, il comma 2-*duodecies*, secondo il quale la verifica dell'identità digitale con livello di garanzia almeno significativo ai sensi dell'art.8, paragrafo 2, del Regolamento eIDAS, produce, nelle transazioni elettroniche o per l'accesso ai servizi in rete, gli effetti del documento di riconoscimento equipollente ai sensi dell'art.35 del Decreto del Presidente della Repubblica 28 dicembre 2000 n.445. A tal riguardo, sembrerebbe sussistere un difetto di coordinamento tra le normative sopra richiamate in quanto il citato art.35 del DPR 445/2000 , interpretato sistematicamente, parrebbe riconoscere l'equipollenza di documenti alternativi alla carta di identità a condizione che questi siano dotati di una fotografia del soggetto, elemento di cui SPID è ad oggi sprovvisto.

Da quanto precede ne deriva che SPID e CIE, pur essendo strumenti molto diversi tra loro, sebbene, come detto, appartenenti alla più ampia categoria delle identità digitali, sembrano destinati ad essere sostanzialmente equiparati ai fini dell'identificazione personale nell'ambito dell'identificazione a distanza dell'utente. Non a caso, sia SPID[56] che la CIE[57] (nell'ordine) sono stati entrambi oggetto, da parte dello Stato italiano, di notifica ai sensi dell'art. 9 del regolamento UE 910/2014, quali mezzi di identificazione elettronica destinati ad essere riconosciuti nei rapporti con gli altri Paesi membri.

Proseguendo con i distinguo, rimane da dire che l'autenticazione si differenzia anche dalla sottoscrizione elettronica in quanto quest'ultima non è utile, a differenza della prima, alla fruizione di risorse o contenuti erogati su un portale, ma a prestare adesione al contenuto

55 I documenti di identità, sia analogici che elettronici, vanno infatti sempre richiesti al proprio Comune di residenza o di dimora, e per i cittadini residenti all'estero presso il Consolato.
56 Gazzetta Ufficiale Unione Europea del 10 settembre 2018.
57 Gazzetta Ufficiale Unione Europea del 13 settembre 2019.

di un determinato documento al fine di conferire allo stesso un determinato valore giuridico nei rapporti con altri soggetti. A sua volta la sottoscrizione elettronica si differenzia dalla identificazione personale in quanto quest'ultima non è idonea ad essere valutata di per sé quale sintomo di adesione ad un documento e di converso, la sottoscrizione elettronica, non è idonea di per sé ad identificare un soggetto non contenendo necessariamente alcun riferimento a dati biometrici dello stesso e mancando degli altri requisiti tipici dei mezzi di identificazione personale sopra delineati[58].

Ma anche sotto questo aspetto il legislatore non ha mancato di creare pericolose equiparazioni quando, come già visto, ai sensi dell'art. 11 del Regolamento recante le modalità attuative per la realizzazione dello SPID, ha stabilito che l'identificazione informatica ai fini del rilascio dell'identità SPID può avvenire tramite firma elettronica qualificata o firma digitale.

Pertanto, SPID, alla luce delle norme appena richiamate, seppur al netto delle considerazioni precedentemente svolte, può essere definito come un sistema di carattere ibrido disciplinato da una normativa alquanto ondivaga spesso piegata ad una visione "commerciale" che tende a premiare i grandi enti privati (Banche e grandi Telcom *in primis*). La commistione di interessi pubblici e privati ha nella sostanza finito per confondere piani e livelli di ragionamento del tutto differenti tra loro, travolgendo principi relativi all'accertamento dell'identità personale tradizionali ormai assodati in nome di una "fuga in avanti" che il legislatore tecnico italiano sembra aver intrapreso da qualche tempo.

In ogni caso, tutti questi aspetti, come visto, rappresentano un tema molto presente sul tavolo delle istituzioni competenti. Come detto in precedenza, l'emendamento 42.24 al decreto legge 30 dicembre 2019 n.162, presentato dal Governo, e poi ritirato, proponeva, infatti, di modificare pesantemente la normativa precedente in quanto tentava di intervenire nella materia prevedendo che lo Stato diventasse *Identity Provider* unico, oltre alla abrogazione del sistema SPID ed alla sua sostituzione con l'identità digitale abbinata al rilascio della carta di identità elettronica. Essendo, al momento in cui si scrive, in corso l'*iter* di conversione in legge, non è affatto esclusa una eventuale riproposizione di un nuovo emendamento con contenuti analoghi.

58 Infatti, ai sensi dell'art. 20, comma 1-*bis* del CAD, il documento informatico soddisfa il requisito della forma scritta ed ha l'efficacia prevista dall'art.2702 c.c. quando (…) è formato, previa identificazione informatica del suo autore, attraverso un processo avente requisiti (…) tali da garantire la sicurezza, integrità ed immodificabilità del documento e, in maniera manifesta ed inequivoca, la sua riconducibilità all'autore. La norma pertanto non si limita a prendere in considerazione la semplice apposizione di una firma digitale, ma pone l'accento sull'identificazione del soggetto che sottoscrive digitalmente, definendola per l'appunto "un processo".

10) SPID come mezzo di identificazione nella nuova "SRL *online*"?

Con la Direttiva (UE) 2019/1151, pubblicata nella GUCE del giorno 11 luglio 2019, l'Unione Europea ha avviato definitivamente un percorso che, in futuro, dovrebbe portare verso un diritto societario unico e digitale.

La citata Direttiva pone un termine agli Stati membri di predisporre una infrastruttura che consenta la costituzione di società a responsabilità limitata (srl e srls) mediante mezzi informatici. Lo scopo della Direttiva in parola è quello di consentire ai cittadini degli Stati membri di poter costituire società a distanza in modo da favorire il commercio e l'economia comuni[59].

Più precisamente, a decorrere dalla data di entrata in vigore (31 luglio 2019), gli Stati membri hanno due anni di tempo per recepire le disposizioni nel proprio diritto nazionale. Il suddetto termine può essere prorogato di un altro anno in caso di particolari difficoltà nel recepimento[60]. Pertanto, al più tardi entro la metà del 2021, la costituzione *online* diverrà realtà in tutti gli Stati membri.

In realtà, in Italia la costituzione con procedura telematica non è una novità assoluta, in quanto essa è già prevista limitatamente alle sole Srl *Start-up* innovative di cui all'art. 25, comma 2, D.L. n.179/12.

Per consentire il corretto espletarsi delle procedure di costituzione, viene stabilito che l'identificazione dei soggetti intervenuti a tal fine debba avvenire a distanza con mezzi che assicurino l'assenza di frodi e furti di identità. Viene ammessa a tal riguardo anche la identificazione a mezzo di sistemi audio-video che consentano l'identificazione sicura del soggetto.

L'elemento centrale delle nuove norme in commento, quantomeno ai fini che qui ci interessano, è, pertanto, l'identificazione dei richiedenti mediante la procedura di autenticazione a norma del Reg. UE n.910/2014 (eIDAS). Proprio sotto il profilo dell'identificazione, è stabilito che i legislatori, nel recepimento della direttiva, devono concentrarsi sull'uso efficace dei meccanismi di protezione previsti dalla stessa, mantenendo al minimo il rischio di abusi. Inoltre, ai sensi dell'art. 6 del regolamento eIDAS, ogni Stato membro ha il dovere di riconoscere i sistemi di identificazione elettronica degli altri Stati membri, da questi notificati alla Commissione e pubblicati nell'elenco previsto dall'art. 9 del Regolamento. Si ricorda, al riguardo che l'Italia ha notificato finora, quali strumenti di identificazione elettronica, sia SPID che CIE.

Ad oggi, l'applicazione della suddetta Direttiva appare assai problematica sotto diversi punti di vista. Da un lato, si è messo fortemente in dubbio la compatibilità dei sistemi di

59 Essa fa parte del c.d. *Company Law Package*, che comprende anche una direttiva sulle trasformazioni, fusioni e scissioni transfrontaliere.
60 Art.2, comma 1, della Direttiva.

identificazione a distanza con i criteri tipici di un registro delle imprese affidabile[61]: mancherebbero, infatti, norme uniformi in materia di controllo, sicurezza e registrazione dei mezzi elettronici di identificazione. Altro elemento non trascurabile è rappresentato dal fatto che secondo il Regolamento eIDAS una procedura di identificazione elettronica non è in grado di rivelare l'identità della persona che agisce effettivamente: anche se la procedura è tecnicamente priva di errori, la rappresentanza indiretta da parte di prestanomi, la minaccia, la coercizione e l'incapacità d'agire non vengono rilevate[62]. Neanche un'ipotetica applicazione ai registri pubblici della tanto discussa tecnologia Blockchain[63] eliminerebbe questi pericoli, in quanto il rischio per la sicurezza si annida nel momento di ingresso nel sistema e non nella semplice trasmissione o registrazione delle informazioni[64].

Sotto tali aspetti, proprio la Direttiva in commento, al fine di prevenire il rischio di abusi derivante dall'avvio obbligatorio della procedura di identificazione, lascia agli Stati membri la possibilità di elaborare meccanismi supplementari consentendo di adottare mezzi e metodi ulteriori per effettuare tali controlli. Invero, proprio sotto tale aspetto la Direttiva non prende posizione circa la presenza o meno della figura del Notaio durante la fase della costituzione della società, ma al contempo essa lascia, tuttavia, la possibilità agli Stati membri di stabilire, in conformità alle rispettive normative, se la costituzione debba avvenire, in determinate ipotesi[65], in presenza fisica di un pubblico ufficiale o di una pubblica autorità[66]. Inoltre, il comma 4, lett. c) dell'art. 13 *octies* specifica che le disposizioni nazionali possono richiedere in tutte le fasi della procedura *online* l'intervento di un

---

61 KINDLER, Gesellschaftsrecht im Zeitalter der Digitalisierung, in SCHNAUDER, Digitalisierung im Gesellschaftsrecht, Wien, 2018, pp. 39, 54.

62 KINDLER, Unternehmen im Binnenmarkt cit., p. 86; WOLF, Grenzuberschreitende Mobilitat von Gesellschaften in Europa, in Mitteilungen des Bayerischen Notarvereins, 2018, pp. 510, 522; BORMANN e STELMASZCZYK, op. cit., p. 609.

63 Vedasi, al riguardo PAULUS e MATZKE, Smart Contracts und das BGB. Viel Larm um nichts?, in Zeitschrift fur die gesamte Privatrechtswissenschaft, 2018, pp. 431, 436.

64 Cfr. SPINDLER, Gesellschaftsrecht und Digitalisierung, in Zeitschrift fur Unternehmens und Gesellschaftsrecht, 2018, pp. 17, 49 ss.; SATTLER, Der Einfluss der Digitalisierung auf das Gesellschaftsrecht, in Betriebs-Berater, 2018, pp. 2243, 2245; in modo analogo, si esprime anche la dottrina italiana: C. LICINI, *Il notaio dell'era digitale: riflessioni gius-economiche*, in Notariato IPSOA, 2018. Cfr. anche M. Manente, *Blockchain: la pretesa di sostituire il notaio*, Notariato IPSOA, 2016 e M. Nastri, *Registri sussidiari, Blockchain: #notaio oltre la lezione di Carnelutti?*, Notariato IPSOA, 2017.

65 In base alla premessa 21 della Direttiva, "ove sia giustificato da ragioni di interesse pubblico intese ad impedire l'usurpazione o l'alterazione di identità, o a garantire il rispetto delle norme in materia di capacità giuridica e di autorità dei richiedenti a rappresentare una società, agli Stati membri dovrebbe essere consentito adottare misure, in conformità al diritto nazionale, che potrebbero richiedere la presenza fisica del richiedente dinnanzi a un'autorità, a una persona o a un organismo incaricato a norma del diritto nazionale di trattare ogni aspetto delle procedure online, dello Stato membro in cui si intende costituire la società o registrare la succursale. Tuttavia tale presenza fisica non dovrebbe essere richiesta in modo sistematico, ma solo caso per caso, se vi sono motivi di sospettare la falsificazione dell'identità del richiedente o il mancato rispetto delle norme riguardanti la capacità giuridica e la capacità dei richiedenti a rappresentare una società. Il sospetto dovrebbe essere basato su informazioni a disposizione delle autorità o delle persone o degli organismi incaricati, a norma delle leggi nazionali, di effettuare tale tipo di controlli. Qualora sia richiesta la presenza fisica, gli Stati membri, dovrebbero garantire che ogni altra fase della procedura possa essere completata online. Il concetto di capacità giuridica dovrebbe essere inteso come comprensivo della capacità di agire.".

66 Principio già espresso anche nell'art. 10 della dir. 2017/1132 UE.

notaio[67] incaricato "di trattare per qualsiasi aspetto della costituzione online della società". Pertanto, alla luce di quanto detto, la presenza del notaio potrebbe essere prevista tanto per le limitate ipotesi in cui sia necessaria la presenza fisica del richiedente, quanto nella generalità delle costituzioni *online*.

Appare, pertanto, chiaro come sia altamente auspicabile che il legislatore italiano sfrutti positivamente tali riserve la quale rappresenterebbe l'unica soluzione in grado di assicurare il non proliferare di incertezze, truffe ed abusi dovuti all'utilizzo di mezzi di identificazione a distanza. La presenza del Notaio, infatti, non solo avrebbe l'effetto di proteggere l'integrità dei pubblici registri, ma anche di assicurare l'importante funzione antiprocessualistica, essendo probabilmente, la figura notarile, l'unica in grado di compensare le carenze di sicurezza della procedura di identificazione elettronica secondo il regolamento eIDAS.

11) Conclusioni.

Il Sistema Pubblico di Identità Digitale (SPID) rappresenta sicuramente un elemento innovativo e di avanguardia per la fruizione dei servizi offerti dalla Pubblica Amministrazione. Il processo di informatizzazione dei servizi pubblici, infatti, appare un tema sempre più decisivo e centrale sia in ambito nazionale che europeo, con rilevanza sia economica che sociale.

Con i suoi tre livelli di sicurezza, SPID è in grado di garantire una autenticazione con un adeguato livello di protezione in relazione al servizio di cui si intende fruire ed al rischio ad esso conseguente, consentendo quindi, a differenza del passato, di eseguire operazioni complesse e rischiose anche da remoto.

La recente implementazione dello SPID Professionale ha, inoltre, aperto la strada alle identità digitali qualificate, fondamentali per accelerare il processo di integrazione tra l'attività dei professionisti e delle persone giuridiche, con le pubbliche amministrazioni.

SPID porta con sé anche la possibilità di inviare e ricevere comunicazioni nei confronti della Pubblica Amministrazione e, in combinazione con la PEC, è in grado di costituire un vero e proprio domicilio digitale destinato, in futuro, a confluire nella Anagrafe della Popolazione Residente.

Infine SPID, sulla base delle più recenti novità normative, è divenuto anche mezzo di identificazione a distanza valido sia ai fini antiriciclaggio sia ai fini delle transazioni elettroniche. E sotto tale ambito, sulla base di quanto stabilito dalla Direttiva (UE) 2019/1151, in tema di SRL *online*, SPID, insieme alla CIE, diventerà uno degli elementi di identificazione personale del comparente connesso in remoto.

67 Cfr. il ventesimo considerando.

Tuttavia, al netto delle considerazioni precedenti, in questo momento storico di radicali trasformazioni sociali e culturali, serve una grande attenzione da parte del Legislatore al fine di evitare pericolose fughe in avanti e fantasiose equiparazioni che rischiano di essere portatrici di profonde incertezze che potrebbero riverberarsi, in un futuro non troppo lontano, anche nell'ambito della contrattazione. Le scelte finora adottate appaiono spesso frutto da un lato di un giustificabile desiderio di sburocratizzare i processi innovandoli, dall'altro di scelte eccessivamente mercatiste che hanno portato a delegare vitali funzioni dello Stato (quale è quella relativa al rilascio di mezzi di identificazione personale) ai grandi *players* economici. In mezzo a questi ultimi elementi c'è anche l'aspetto relativo alla tecnica legislativa, la quale, essendo troppo votata all'ascolto delle esigenze informatiche piuttosto che di quelle giuridiche, sta lentamente affermando una egemonia della tecnica ai danni del diritto.