

Agenda digitale: il sistema Spid e l'Anagrafe nazionale della popolazione residente

ABSTRACT

La circolare illustra la disciplina generale e le disposizioni attuative del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) e dell'Anagrafe nazionale della popolazione residente (Anpr). L'infrastruttura Spid e la piattaforma dell'Anpr sono due dei principali obiettivi della "Strategia per la crescita digitale 2014-2020".

Lo Spid è uno strumento volto a consentire un accesso agevole di cittadini e imprese ai servizi in rete delle pubbliche amministrazioni e delle imprese che aderiranno al sistema. Esso prevede tre diversi livelli di sicurezza, come richiesto dal nuovo regolamento europeo sull'identificazione elettronica (regolamento eIDAS). Lo Spid è destinato ad essere lo strumento fondamentale per l'interazione on line con le pubbliche amministrazioni, anche se permane la possibilità di utilizzare a tal fine la Carta nazionale dei servizi e la Carta d'identità elettronica (per la quale sono state definite le caratteristiche tecniche ed è stato avviato un piano graduale di rilascio da parte dei comuni).

Lo Spid è stato elaborato alla luce del regolamento europeo sull'identificazione elettronica (regolamento eIDAS), tenendo conto dell'esigenza di assicurare l'interoperabilità del sistema nel contesto tecnologico europeo. In prospettiva lo Spid potrà essere utilizzato per accedere ai servizi pubblici on line negli altri Stati membri, nel rispetto di una serie di condizioni previste dal regolamento eIDAS. Alcuni gestori di identità digitale si sono già accreditati nel registro Spid ed alcune amministrazioni pubbliche da gennaio 2016 consentono l'accesso ai propri servizi in rete tramite il nuovo sistema.

L'Anagrafe nazionale della popolazione residente supera il sistema delle anagrafi comunali, realizzando un'unica banca dati a cui possono fare riferimento i comuni, le altre pubbliche amministrazioni, i gestori dei pubblici servizi e i cittadini interessati. Il processo di subentro dei comuni nell'Anpr è iniziato a dicembre 2015 e dovrebbe completarsi entro la fine del 2016.

PROVVEDIMENTI COMMENTATI

Capo II del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 (regolamento eIDAS sull'identificazione elettronica)

Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 (Spid)

Decreto del Presidente del Consiglio dei Ministri 10 novembre 2014, n. 194 (Anpr)

Articolo 10 del decreto legge 19 giugno 2015, n. 78, convertito dalla legge 6 agosto 2015, n. 125 (Anpr)

Regolamenti di attuazione dello SPID emanati dall'Agenzia per l'Italia digitale con determinazione n. 44/2015 del 28 luglio 2015

Decreto del Ministero dell'Interno 23 dicembre 2015 (carta d'identità elettronica)

INDICE

Introduzione	p. 5
1. Lo Spid alla luce del Regolamento europeo in materia di identificazione elettronica	p. 6
2. La disciplina nazionale dello Spid	p. 9
2.1 Le disposizioni del Cad	p.10
2.2 Il decreto 24 ottobre 2014 e i regolamenti attuativi	p.12
3. L'Anagrafe nazionale della popolazione residente	p.22
3.1 Le disposizioni del Cad	p.23
3.2 Il decreto del Presidente del Consiglio dei Ministri n. 194/2014	p.24

Introduzione

La realizzazione del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) e l'istituzione dell'Anagrafe nazionale della popolazione residente (Anpr) costituiscono due dei principali obiettivi dell'Agenda digitale in Italia, come delineata da ultimo dalla "Strategia per la crescita digitale 2014-2020"¹. Lo Spid è un'infrastruttura critica di base volta a consentire ai cittadini e alle imprese un accesso sicuro e protetto, anche in mobilità, ai servizi digitali della pubblica amministrazione e dei soggetti privati che aderiranno al sistema. L'obiettivo è quello di stimolare la domanda di servizi on line da parte di cittadini e imprese. L'Anpr è invece una delle piattaforme abilitanti (come, ad esempio, i pagamenti elettronici e la fatturazione elettronica della PA) realizzate seguendo la logica del *Digital first* e volte a favorire lo sviluppo di servizi digitali innovativi.

Sia lo Spid che l'Anpr sono previsti dal codice dell'amministrazione digitale (Cad)². La disciplina dell'Anpr contenuta nel Cad è stata oggetto di alcune modifiche con il decreto legge 19 giugno 2015, n. 78, convertito dalla legge 6 agosto 2015, n. 125. Per lo Spid, la legge 7 agosto 2015, n. 124, che contiene deleghe al Governo in materia di riorganizzazione delle pubbliche amministrazioni (cosiddetta 'legge Madia'), prevede entro agosto 2016 un intervento di modifica e integrazione del Cad volto tra l'altro a coordinare e razionalizzare le disposizioni legislative in materia di strumenti di identificazione, comunicazione e autenticazione in rete con la disciplina relativa allo Spid, anche al fine di promuovere l'adesione a questo sistema.

Di recente sono stati adottati, sia per lo Spid che per l'Anagrafe nazionale, i provvedimenti attuativi necessari per passare alla fase operativa.

Con riferimento allo Spid, il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 ha definito le caratteristiche del sistema ed è stato seguito nel luglio 2015 dall'adozione da parte dell'Agenzia per l'Italia digitale di quattro regolamenti attuativi dedicati rispettivamente: 1) alle regole tecniche; 2) alle modalità attuative per la realizzazione dello Spid; 3) alle modalità di accreditamento dei soggetti Spid; 4) alle

¹ La "Strategia per la crescita digitale 2014-2020" è stata approvata dalla Presidenza del Consiglio dei Ministri il 3 marzo 2015 (http://www.governo.it/sites/governo.it/files/strategia_crescita_digitale.pdf).

² Decreto legislativo 7 marzo 2005, n. 82.

procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di sistemi preesistenti di identificazione informatica conformi ai requisiti dello Spid, il rilascio dell'identità digitale.

Riguardo all'Anagrafe nazionale della popolazione residente il decreto del Presidente del Consiglio dei Ministri 10 novembre 2014, n. 194 ha definito le modalità di funzionamento e il piano per il graduale subentro dell'Anpr alle anagrafi comunali.

Questa circolare illustra anzitutto la nuova disciplina europea dell'identificazione elettronica nell'ambito della quale si colloca lo Spid, per poi analizzare l'attuale disciplina nazionale con riferimento sia allo Spid che all'Anpr.

1. Lo Spid alla luce del Regolamento europeo in materia di identificazione elettronica

Lo Spid va visto alla luce della nuova disciplina europea dell'identificazione elettronica e dei servizi fiduciari contenuta nel regolamento (UE) n. 910/2014 (cosiddetto regolamento eIDAS)³, che a partire dal 1° luglio 2016 abroga la direttiva 1999/93/CE sulle firme elettroniche. Trattandosi di un regolamento, la nuova disciplina europea è direttamente applicabile negli Stati membri senza necessità di un recepimento a livello nazionale.

Per identificazione elettronica, il regolamento eIDAS intende il processo per cui si fa uso di dati di identificazione personale⁴ in forma elettronica che rappresentano un'unica persona fisica o giuridica, o una persona fisica in rappresentanza di una persona giuridica⁵.

Nel Capo II dedicato all'identificazione elettronica il regolamento fissa le condizioni a cui gli Stati membri sono tenuti ad assicurare il mutuo riconoscimento dei mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime di identificazione elettronica di un altro Stato membro (artt. 6-9)⁶.

³ Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

⁴ Per dati di identificazione personale si intende un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica o di una persona fisica che rappresenta una persona giuridica.

⁵ Regolamento eIDAS, articolo 3.

In base al regolamento, gli Stati membri sono liberi di stabilire quali strumenti di identificazione elettronica utilizzare per l'accesso ai servizi on line nel proprio territorio e non hanno l'obbligo di notificare i loro regimi di identificazione alla Commissione. La notifica alla Commissione è però necessaria per ottenere il mutuo riconoscimento del mezzo di identificazione elettronica per l'accesso on line ai servizi pubblici in altri Stati membri.

Più in particolare, l'articolo 7 del regolamento eIDAS indica alcune condizioni che devono essere soddisfatte affinché un regime di identificazione elettronica possa essere notificato alla Commissione:

- i mezzi di identificazione elettronica nell'ambito del regime sono rilasciati dallo Stato notificante o su suo incarico o comunque essere da esso riconosciuti;
- il regime e i mezzi di identificazione elettronica rilasciati in base alle sue disposizioni soddisfano i requisiti di almeno uno dei livelli di garanzia (basso, significativo o elevato) disciplinati dall'articolo 8 e dal regolamento di esecuzione (UE) 2015/1502 della Commissione dell'8 settembre 2015 sulle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica;
- lo Stato notificante e la parte che rilascia i mezzi di identificazione elettronica garantiscono, nell'ambito delle rispettive competenze, la conformità al pertinente livello di garanzia;
- lo Stato notificante garantisce la disponibilità dell'autenticazione on line per consentire alle parti stabilite in un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica⁷;
- il regime soddisfa inoltre i requisiti definiti dal regolamento di esecuzione (UE) n. 2015/1501 della Commissione dell'8 settembre 2015 relativo al quadro di interoperabilità.

⁶ I mezzi di identificazione elettronica sono unità materiali e/o immateriali contenenti dati di identificazione personale utilizzate per l'autenticazione per un servizio on line. Per 'regime di identificazione elettronica' si intende un sistema di identificazione elettronica per cui si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche o alle persone fisiche che rappresentano persone giuridiche.

⁷ Per 'autenticazione' si intende il processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica oppure l'origine e l'integrità di dati in forma elettronica (regolamento eIDAS, articolo 3).

L'articolo 9 indica le modalità della notifica e prevede che, un anno dopo la data di applicazione degli atti di esecuzione del regolamento (UE) 2015/1502, la Commissione pubblichi un elenco dei regimi di identificazione elettronica notificati⁸. Le notifiche ricevute successivamente verranno aggiunte all'elenco entro due mesi dalla loro ricezione.

La disciplina del mutuo riconoscimento è contenuta nell'articolo 6 del regolamento. Quando un ordinamento nazionale richiede l'impiego di un'identificazione elettronica per accedere a un servizio prestato da un organismo del settore pubblico on line in uno Stato membro, i mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti nel primo Stato ai fini dell'autenticazione transfrontaliera di tale servizio on line se sono rispettate le seguenti condizioni:

- a. i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime pubblicato nell'elenco;
- b. il livello di garanzia dei mezzi di identificazione elettronica corrisponde a un livello pari o superiore al livello richiesto dall'organismo pubblico dello Stato in cui è richiesto l'accesso al servizio on line in questione (ed è significativo o elevato);
- c. l'organismo del settore pubblico competente utilizza un livello di garanzia significativo o elevato in relazione all'accesso al servizio on line.

Per i mezzi di identificazione elettronica rilasciati nell'ambito di un regime di identificazione compreso nell'elenco corrispondenti al livello di garanzia basso, gli Stati membri non hanno l'obbligo, ma solo la facoltà, del mutuo riconoscimento ai fini dell'autenticazione transfrontaliera (articolo 6, paragrafo 2).

I restanti articoli del Capo II del regolamento eIDAS disciplinano, rispettivamente, gli obblighi dello Stato notificante in caso di violazione o parziale compromissione del regime di identificazione elettronica notificato (articolo 10), il regime delle responsabilità in caso di danni causati per dolo o negligenza a persone fisiche o giuridiche in seguito al mancato adempimento degli obblighi previsti dalla disciplina in una transazione transfrontaliera (articolo 11) e, infine, le condizioni di interoperabilità che devono essere soddisfatte dai regimi di identificazione elettronica notificati e gli obblighi di

⁸ Almeno sei mesi prima della notifica alla Commissione, lo Stato membro notificante fornisce agli altri Stati membri una descrizione del regime, in attuazione dell'obbligo di cooperazione in tema di interoperabilità e sicurezza.

cooperazione tra gli Stati membri per quanto riguarda l'interoperabilità e la sicurezza dei regimi (articolo 12)⁹.

Lo SPID è stato elaborato alla luce delle disposizioni del regolamento eIDAS, tenendo in particolare considerazione l'esigenza di assicurare l'interoperabilità del sistema nel contesto tecnologico europeo¹⁰. L'inserimento dello Spid nell'elenco dei regimi notificati alla Commissione quali sistemi di identificazione elettronica conformi al regolamento eIDAS porterà al suo riconoscimento per l'accesso ai servizi pubblici on line negli altri Stati membri, alle condizioni indicate dall'articolo 6 del regolamento.

2. La disciplina nazionale dello Spid

Il sistema Spid costituisce uno strumento per l'accesso da parte di cittadini e imprese ai servizi in rete per i quali sia necessaria l'identificazione informatica.

Già da tempo le pubbliche amministrazioni e i privati consentono l'accesso ai servizi in rete mediante varie forme di identificazione informatica. Tuttavia gli strumenti rilasciati a tal fine dai soggetti sia pubblici che privati erano sinora generalmente utilizzabili da cittadini e imprese solo per l'accesso ai servizi resi disponibili dal soggetto che li forniva. Il sistema Spid è invece volto a consentire ai titolari dell'identità digitale di utilizzare le medesime credenziali per l'accesso in rete a una pluralità di servizi resi disponibili da diversi fornitori.

⁹ Sull'interoperabilità, cfr. il già citato regolamento di esecuzione (UE) n. 2015/1501 della Commissione.

¹⁰ Lo SPID si basa su specifiche tecniche molto diffuse a livello europeo (OASIS SAML v2.0) e adottate nel progetto sperimentale Stork, che mira a sviluppare un'infrastruttura comune per l'identità digitale. Lo schema di decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 che attua lo Spid, era stato notificato alla Commissione europea ai sensi della direttiva 98/34/CE, come modificata, relativa ad "una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relativi ai servizi della società dell'informazione" (notifica 2014/295/I del 23 giugno 2014). Per l'inserimento nell'elenco previsto dal regolamento eIDAS occorre una distinta notifica, volta a consentire alla Commissione di verificare la conformità del sistema Spid al regolamento.

2.1 Le disposizioni del Cad

Il Cad dedica una specifica disposizione (articolo 64) alle modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni. Come anticipato, con l'attuazione della legge Madia verranno apportate alcune modifiche a questa disposizione.

L'attuale formulazione dell'articolo 64 Cad prevede anzitutto che la carta d'identità elettronica (CIE) e la carta nazionale dei servizi (CNS) costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica. In aggiunta a questi strumenti, per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese anche in mobilità, l'articolo 64, comma 2-bis prevede l'istituzione dello Spid a cura dell'Agenzia per l'Italia digitale (Agid)¹¹.

Lo Spid, una volta istituito, rappresenta l'unico strumento alternativo alla CIE e alla CNS per l'accesso ai servizi in rete erogati dalle pubbliche amministrazioni. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni¹².

In base al Cad, lo Spid è costituito come un insieme aperto di soggetti pubblici e privati che, previo accreditamento presso l'Agenzia per l'Italia digitale (Agid), gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese.

Per le pubbliche amministrazioni l'adesione allo Spid è obbligatoria¹³. Per le imprese, invece, avvalersi dello Spid al fine di erogare i propri servizi in rete è una facoltà. Il Cad prevede che l'impresa che aderisce allo Spid per la verifica dell'accesso ai servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente non è tenuta a un obbligo generale di sorveglianza delle attività sui propri siti ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70, sul commercio elettronico¹⁴.

¹¹ L'Agid è stata istituita dal decreto legge 22 giugno 2012, n. 83, convertito dalla legge 7 agosto 2012, n. 134, e successive modifiche (articoli da 19 a 22).

¹² Cad, articolo 64, comma 2.

¹³ Cad, articolo 64, comma 2-quater.

¹⁴ L'articolo 17 del decreto legislativo n. 70/2003 identifica i servizi della società dell'informazione per i quali il prestatore non è assoggettato a un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

In attuazione delle disposizioni del Cad¹⁵, le caratteristiche del sistema Spid, i tempi e le modalità per la sua adozione da parte delle pubbliche amministrazioni e le modalità con cui le imprese potranno avvalersi del sistema sono state definite con un decreto del Presidente del Consiglio dei ministri, adottato il 24 ottobre 2014, che verrà analizzato nel prossimo paragrafo.

Per quanto riguarda le previste modifiche del Cad, l'articolo 1 della legge n. 124/2015 delega il Governo all'adozione di uno o più decreti legislativi volti a garantire ai cittadini e alle imprese il diritto di accedere facilmente a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale ('Carta della cittadinanza digitale'). La legge delega prevede a questo fine interventi di modifica e integrazione del Cad, anche attraverso la delegificazione. Tra i criteri della delega presenta particolare rilievo in questa sede quello del coordinamento e della razionalizzazione delle vigenti disposizioni di legge in materia di strumenti di identificazione, comunicazione e autenticazione in rete con la disciplina di cui all'articolo 64 del Cad e la relativa normativa di attuazione in materia di Spid, anche "al fine di promuovere l'adesione da parte delle amministrazioni pubbliche e dei privati" allo Spid¹⁶.

Il decreto legislativo di attuazione dell'articolo 1 della legge Madia è stato approvato in prima lettura dal Consiglio dei ministri del 20 gennaio 2016¹⁷. Lo schema di decreto modifica l'articolo 64 del Cad attribuendo allo Spid un ruolo centrale come strumento per agevolare la diffusione dei servizi in rete e l'accesso agli stessi da parte di cittadini e imprese, pur continuando a prevedere la possibilità di accedere ai servizi erogati in rete dalle pubbliche amministrazioni attraverso la Carta nazionale dei servizi e la Carta di identità elettronica.

A quest'ultimo riguardo segnaliamo che con il decreto del Ministero dell'Interno 23 dicembre 2015 sono state definite le caratteristiche tecniche e le modalità tecniche di emissione, produzione, distribuzione, gestione e supporto all'utilizzo della Carta d'identità elettronica. Il supporto fisico della CIE è realizzato con le tecniche tipiche della produzione di carte valori e integrato con un microprocessore per memorizzare le informazioni necessarie per la verifica dell'identità del titolare¹⁸ nonché per l'autenticazione in rete secondo specifiche caratteristiche tecniche. Dopo l'entrata in

¹⁵ Cad, articolo 64, commi 2-*quater*, 2-*quinqüies* e 2-*sexies*.

¹⁶ Legge n. 124/2015, articolo 1, comma 1, lettera f).

¹⁷ Il testo è disponibile al seguente link:
<http://www.funzionepubblica.gov.it/comunicazione/notizie/2016/gennaio/riforma-pa-approvati-i-primi-11-decreti-attuativi.aspx>.

¹⁸ Inclusi elementi biometrici primari (immagini del volto) e secondari (impronte digitali).

vigore del decreto, avvenuta il 30 dicembre 2015, i Comuni procederanno al rilascio delle CIE secondo un piano graduale, definito dall'articolo 14 del decreto.

2.2 Il decreto 24 ottobre 2014 e i regolamenti attuativi

Il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, emanato ai sensi dell'articolo 64 del Cad, definisce le caratteristiche dello Spid, i tempi e le modalità di adozione del sistema da parte delle pubbliche amministrazioni e le modalità attraverso cui le imprese possono avvalersi del sistema Spid per la gestione dell'identità digitale dei propri utenti.

In attuazione del decreto, il 28 luglio 2015 l'Agid ha emanato quattro regolamenti. I primi due regolamenti definiscono le regole tecniche e le modalità attuative per la realizzazione dello Spid; il terzo regolamento contiene le modalità di accreditamento dei soggetti che partecipano allo Spid e il quarto regolamento prevede le procedure per consentire il rilascio, da parte dei gestori, dell'identità digitale attraverso l'utilizzo di sistemi preesistenti di identificazione informatica conformi ai requisiti dello Spid.

Finalità dello Spid e soggetti partecipanti

Come anticipato, lo Spid è il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese. Il decreto definisce l'identità digitale 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"¹⁹.

La finalità dello Spid è di consentire agli utenti di avvalersi di gestori dell'identità digitale e di gestori di attributi qualificati per consentire ai fornitori di servizi l'immediata verifica della loro identità e di eventuali attributi qualificati (ad esempio qualifiche, abilitazioni professionali o poteri di rappresentanza²⁰) che li riguardano.

I soggetti pubblici o privati che partecipano allo Spid sono i gestori dell'identità digitale, i gestori degli attributi qualificati, i fornitori di servizi, l'Agid e gli utenti. L'insieme di questi soggetti, esclusi gli utenti, costituisce un sistema aperto e cooperante che consente ai partecipanti di comunicare utilizzando meccanismi di interazione, standard

¹⁹ Decreto 24 ottobre 2014, articolo 1, comma 1, lettera o).

²⁰ Decreto 24 ottobre 2014, articolo 1, comma 1, lettera e).

tecnologici e protocolli indicati nel decreto e precisati nelle regole tecniche definite dall'Agid²¹.

I compiti dell'Agid

In base all'articolo 4 del decreto, l'Agid cura l'attivazione dello Spid e in particolare:

- a) gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni;
- b) cura l'aggiornamento del registro Spid, accessibile al pubblico, che contiene l'elenco dei soggetti abilitati a operare in qualità di gestori dell'identità digitale, di gestori degli attributi qualificati e di fornitori di servizi;
- c) vigila sull'operato dei soggetti che partecipano allo Spid, anche con la possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate;
- d) stipula apposite convenzioni con i soggetti che, in base alla disciplina, attestano in quanto fonti istituzionali la validità degli attributi identificativi e consentono la verifica dei documenti d'identità (ad esempio, l'Agenzia delle entrate per la verifica del codice fiscale e dei dati anagrafici ad esso strettamente correlati)²².

Attributi dell'identità digitale e livelli di sicurezza

L'utente può disporre di una o più identità digitali. Ogni identità digitale rilasciata all'utente contiene obbligatoriamente alcune informazioni. Esse sono:

- il codice identificativo, ossia il particolare attributo assegnato dal gestore dell'identità digitale che consente di individuare univocamente un'identità digitale nell'ambito dello Spid²³;
- gli attributi identificativi, che per le persone fisiche sono nome, cognome, luogo e data di nascita, sesso, codice fiscale, estremi di un valido documento d'identità, mentre per le persone giuridiche sono ragione o denominazione

²¹ Decreto, articolo 3;

²² Regolamento Agid sulle modalità attuative, articolo 12.

²³ Il codice identificativo è composto da un codice di quattro lettere e da un codice alfanumerico composto da dieci caratteri (regolamento Agid sulle modalità attuative, articolo 14).

sociale, sede legale, codice fiscale o partita iva, visura camerale attestante lo stato di rappresentante legale del soggetto richiedente l'identità per conto della società e gli estremi del documento d'identità utilizzato dal rappresentante legale²⁴;

- almeno un attributo secondario che serve per le comunicazioni tra il gestore dell'identità digitale e l'utente. In base al decreto del 24 ottobre gli attributi secondari sono il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale ed eventuali altri attributi individuati dall'Agid funzionali alle comunicazioni²⁵. Il regolamento sulle modalità di attuazione dello Spid specifica che per gli attributi secondari devono essere forniti almeno un indirizzo di posta elettronica e un recapito di telefonia mobile. I gestori devono accertare che l'indirizzo di posta elettronica comunicato sia unico in ambito Spid, ossia non sia stato precedentemente indicato per l'acquisizione di un'identità digitale²⁶.

Il decreto prevede che lo Spid è basato su tre livelli di sicurezza delle identità digitali, relativi ai sistemi di autenticazione informatica²⁷.

Nel primo livello il gestore rende disponibili sistemi di autenticazione informatica a un singolo fattore come ad esempio la password. Per il secondo livello Spid il gestore deve rendere disponibili sistemi di autenticazione informatica a due fattori non necessariamente basati su certificati digitali; è accettabile, ad esempio, l'uso di una password e l'adozione di una one time password (OTP) generata con l'ausilio di un dispositivo fisico, l'invio di un sms, liste-tabelle predefinite o applicazioni mobili per smartphone o tablet collegati in rete. Per il terzo livello Spid il gestore deve rendere disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali e criteri di custodia delle chiavi private su dispositivi che soddisfano i requisiti dell'allegato 3 della direttiva 1999/93/CE sulle firme elettroniche²⁸.

L'articolo 6 del decreto specifica che i gestori dell'identità digitale devono garantire che l'autenticazione informatica avvenga attraverso software e soluzioni tecniche che non

²⁴ Decreto 24 ottobre 2014, articolo 1, comma 1, lettera c) e regolamento sulle modalità attuative, articolo 5.

²⁵ Articolo 1, comma 1, lettera d).

²⁶ Regolamento Agid sulle modalità attuative, articolo 5.

²⁷ Per autenticazione informatica il decreto intende la verifica, effettuata dal gestore dell'identità digitale su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'utente allo stesso gestore, al fine di convalidarne l'identificazione informatica.

²⁸ Per maggiori dettagli, cfr. l'articolo 15 del regolamento sulle modalità attuative.

richiedono ai fornitori di servizi di dotarsi di dispositivi, fissi o mobili, proprietari. Sono consentite soluzioni tecniche che prevedono il caricamento del software necessario per effettuare l'autenticazione informatica.

I fornitori di servizi scelgono il livello di sicurezza necessario per l'accesso ai propri servizi tenendo conto delle conseguenze (limitate, serie o severe/catastrofiche) derivanti da un accesso improprio a sistemi o applicazioni. L'Appendice A del regolamento sulle modalità attuative indica che è rilevante sia la circostanza che l'accesso sia solo di tipo informativo oppure consenta di effettuare operazioni dispositive, sia il tipo di informazioni a cui sia accede (ad esempio, dati sensibili, documenti riservati o rilevanti per le amministrazioni e le imprese).

Per rendere omogenei i livelli di sicurezza associati alle diverse categorie di servizi sul territorio nazionale l'Agid è tenuta a promuovere e pubblicare nella sezione Spid del proprio sito istituzionale il livello di sicurezza da associare alle categorie di servizi che presentano carattere di omogeneità.

I gestori dell'identità digitale: accreditamento, obblighi, cessazione dell'attività

Ai sensi del decreto i gestori dell'identità digitale sono le persone giuridiche accreditate allo Spid che, in qualità di gestori di servizio pubblico, dopo l'identificazione certa dell'utente assegnano, rendono disponibili e gestiscono gli attributi utilizzati dall'utente per l'identificazione informatica.

Una sottocategoria dei gestori dell'identità digitale è costituita dai gestori di attributi qualificati. Questi ultimi, previo accreditamento, hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori dei servizi.

Le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale sono specificate nel terzo regolamento dell'Agid, adottato il 28 luglio 2015 e in vigore dal 15 settembre 2015. A partire dal 15 settembre, quindi, è possibile ottenere l'accreditamento come gestori di identità digitale. I riferimenti dei gestori che via via vengono accreditati sono disponibili sul sito dell'Agid²⁹. Uno specifico registro è dedicato ai gestori di attributi qualificati.

L'articolo 10 del decreto indica i requisiti per l'accreditamento dei gestori di identità digitale da parte dell'Agid. Per tutti i gestori, pubblici e privati, sono richiesti capacità organizzativa e tecnica, competenze specifiche del personale, specifiche certificazioni

²⁹ <http://www.agid.gov.it/notizie/2015/12/19/spid-accreditati-i-primi-gestori-identita-digitale>.

e rispetto della normativa sui dati personali; per i privati, inoltre, vi sono requisiti attinenti alla forma giuridica, al capitale sociale e ai requisiti di onorabilità. L'Agid ha il compito di vigilare non solo sul possesso ma anche sulla permanenza di tali requisiti.

Una pronuncia del Tar Lazio del 21 luglio 2015 (n. 2883/2015) ha annullato la previsione che includeva tra i requisiti per l'accreditamento dei gestori il possesso di un capitale sociale non inferiore a cinque milioni di euro, in quanto non ricavabile da alcuna fonte normativa di grado primario, non giustificata dalle caratteristiche tecniche e/o organizzative del servizio e in grado di costituire un significativo ostacolo all'accesso al mercato da parte di imprese dotate delle necessarie competenze³⁰.

L'articolo 10, comma 2, del decreto prevede che dopo l'accoglimento della richiesta di accreditamento, l'Agid informa il richiedente e propone la sottoscrizione di una convenzione. L'iscrizione del gestore nel registro Spid avviene dopo la stipula della convenzione³¹. Ottenuta l'iscrizione nel registro il gestore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni, nel rispetto delle indicazioni della disciplina.

Il gestore Spid deve presentare all'Agid, ai sensi dell'articolo 6, comma 2, del decreto, domanda di autorizzazione all'uso dei sistemi di autenticazione informatica (strumenti, tecnologie, protocolli e quant'altro occorre nel processo di autenticazione). Per quanto attiene alla valutazione di conformità dei sistemi di autenticazione informatica ai livelli di sicurezza di cui all'articolo 6, comma 1, del decreto, è previsto a regime che i gestori si rivolgano a organismi di certificazione appositamente accreditati, sulla base di norme tecniche adottate dall'Agid, che potranno rilasciare rapporti di conformità. L'Agid valuta la rispondenza alle regole tecniche e l'adeguatezza e l'utilizzabilità degli strumenti e delle tecnologie di autenticazione informatica e indica, tenendo conto del rapporto di conformità, il livello di sicurezza corrispondente al sistema di autenticazione informatica notificato.

Il gestore deve pubblicare in un'apposita sezione del proprio sito web, denominata 'soluzioni tecnologiche per l'autenticazione Spid', l'elenco dei sistemi di autenticazione approvati dall'Agid con il livello di sicurezza associato e la relativa data di approvazione.

³⁰ Sulla sentenza n. 2833/2015 è pendente un ricorso davanti al Consiglio di Stato (n. 07008/2015).

³¹ I contenuti del registro Spid relativi a ciascun gestore accreditato sono indicati nella sezione 5 'Contenuti del Registro Spid' del regolamento sulle modalità per l'accreditamento e la vigilanza dei gestori e includono i riferimenti al manuale operativo del soggetto, al manuale utente e la carta dei servizi.

I costi sostenuti dall'Agid per l'attività di vigilanza e accreditamento sono coperti, ai sensi dell'articolo 4, comma 1, lettera a) del decreto, dal contributo dei gestori accreditati. Il regolamento dell'Agid su questi profili specifica che i costi afferenti l'anno solare precedente sono determinati dall'Agid entro il mese di aprile. I costi relativi alla vigilanza per il 50 per cento sono ripartiti tra tutti i gestori attivi presenti nel registro nel corso dell'anno di riferimento e sui gestori revocati o cessati nel medesimo periodo, per il restante 50 per cento sono ripartiti tra gli stessi gestori in misura proporzionale al numero di identità digitali gestite. I costi inerenti le procedure di accreditamento sono ripartiti in ugual misura tra i gestori dell'identità digitale accreditati nello stesso periodo³².

L'articolo 11 indica gli obblighi dei gestori, che riguardano in particolare la garanzia di continuità dei servizi e la sicurezza. Tra gli obblighi attinenti alla sicurezza vi è quello di adottare un piano per la sicurezza dei servizi Spid, secondo le indicazioni fornite dal regolamento Agid (Allegato, parte 3). Inoltre, i gestori sono tenuti a informare tempestivamente l'Agid e il Garante privacy di eventuali violazioni di dati personali.

L'articolo 12 prevede che il gestore che intende cessare l'attività comunichi preventivamente all'Agid questa intenzione indicando gli eventuali gestori sostitutivi o segnalando la necessità di revocare le identità digitali rilasciate. L'eventuale gestore sostitutivo, previo invio all'Agid dell'accettazione della sostituzione e previa acquisizione del consenso degli utenti, subentra nella gestione delle identità digitali rilasciate dal gestore cessato. L'Agenzia, previo accertamento di violazioni della disciplina, può disporre la sospensione dell'attività di attribuzione delle identità da un minimo di un mese a un massimo di un anno e nei casi più gravi la revoca dell'accreditamento del gestore. In quest'ultima circostanza, si applicano le disposizioni sopra illustrate relative alla cessazione dell'attività.

I requisiti per l'accreditamento dei gestori di attributi qualificati sono definiti dall'articolo 16 del decreto. I soggetti che in base alle norme vigenti hanno il potere di attestare gli attributi qualificati devono accreditarsi presso l'Agid indicando i dati che intendono rendere disponibili nello Spid. Le tipologie di dati resi disponibili da ciascun gestore di attributi qualificati sono inserite dall'Agid nell'apposito registro accessibile ai fornitori di servizi. Su richiesta degli interessati sono accreditati di diritto quali gestori di attributi qualificati:

³² Regolamento sull'accreditamento e la vigilanza, sezione 9.

- il Ministero dello sviluppo economico in relazione ai dati contenuti nell'indice nazionale degli indirizzi pec delle imprese e dei professionisti di cui all'articolo 6-bis del Cad;
- i consigli, gli ordini e i collegi delle professioni regolamentate relativamente all'attestazione dell'iscrizione agli albi professionali;
- le camere di commercio per l'attestazione delle cariche e degli incarichi societari iscritti nel registro delle imprese;
- l'Agid in relazione ai dati contenuti nell'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi di cui all'articolo 57-bis del Cad.

Rilascio e gestione delle identità digitali; uso illecito

Il gestore dell'identità digitale, su domanda dell'interessato, rilascia le identità digitali verificando prima l'identità del soggetto richiedente e consegnando in modalità sicura le credenziali di accesso.

In dettaglio, il regolamento sulle modalità attuative specifica che la domanda dell'identità digitale deve essere presentata dal soggetto interessato mediante uno specifico modulo di richiesta di adesione, il cui contenuto è predeterminato³³. Quando riceve la richiesta, il gestore dell'identità digitale procede all'identificazione del soggetto richiedente secondo una delle modalità previste dall'articolo 7 del decreto (a vista, sia in prossimità che da remoto, o attraverso forme di identificazione informatica con un adeguato livello di sicurezza)³⁴. Le modalità di consegna della richiesta e il supporto utilizzato (cartaceo o digitale) dipendono da quale modalità il gestore adotta per il processo di identificazione tra quelle indicate dall'articolo 7 del decreto³⁵.

Dopo aver identificato il soggetto richiedente, il gestore d'identità procede alla verifica dell'identità dichiarata. La verifica, che mira ad aumentare l'attendibilità degli attributi di identità raccolti in fase di identificazione, è svolta attraverso accertamenti presso fonti istituzionali in grado di confermare la veridicità dei dati stessi. L'accesso alle fonti istituzionali ai fini della verifica è effettuato dai gestori in base alle apposite convenzioni previste dall'articolo 4 del decreto. In assenza delle convenzioni, le verifiche sono effettuate sulla base di documenti, dati o informazioni contenuti negli archivi delle amministrazioni competenti, ai sensi dell'articolo 43, comma 2, del testo unico sulla

³³ Regolamento Agid sulle modalità attuative, articolo 5.

³⁴ Sulle varie modalità di verifica dell'identità, cfr. il regolamento sulle modalità attuative, artt. da 6 a 11.

³⁵ Regolamento Agid sulle modalità attuative, articoli 5, 6, 7, 8, 9, 10 e 11.

documentazione amministrativa³⁶. In particolare, i gestori dell'identità digitale e i gestori degli attributi qualificati usufruiscono del servizio di verifica del codice fiscale e dei dati anagrafici ad esso correlati fornito dall'Agenzia delle Entrate³⁷.

Sia il processo di identificazione che il processo di verifica sono eseguiti allo scopo di ottenere un adeguato grado di affidabilità, tenuto conto dello specifico livello di sicurezza nell'ambito dello Spid.

Il processo di registrazione delle informazioni e dei documenti raccolti conclude la fase di rilascio di un'identità Spid. I gestori, per documentare la corretta esecuzione dei processi relativi al rilascio dell'identità, devono conservare la documentazione inerente il processo di adesione per vent'anni dalla scadenza o dalla revoca dell'identità digitale³⁸.

Espletate tutte le attività previste il gestore rilascia l'identità digitale, che è costituita da:

- a) attributi identificativi;
- b) attributi secondari;
- c) codice identificativo;
- d) identificativo utente³⁹.

Il gestore deve a questo punto creare le credenziali che, come anticipato, possono essere di tre tipologie a seconda del livello di sicurezza⁴⁰. La consegna delle credenziali deve avvenire con modalità e strumenti che assicurino che essa sia effettuata al legittimo destinatario, con adeguati criteri di riservatezza che salvaguardino il contenuto⁴¹. Il processo di attivazione delle credenziali, volto a renderle operative e pronte all'utilizzo, è connesso direttamente alla tipologia di credenziali adottate⁴². L'utente può chiedere al gestore dell'identità digitale di segnalargli via mail o sms ogni avvenuto utilizzo delle credenziali di accesso.

³⁶ Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

³⁷ Regolamento Agid sulle modalità attuative, articolo 12.

³⁸ Regolamento Agid sulle modalità attuative, articolo 13.

³⁹ Regolamento Agid sulle modalità attuative, articolo 14.

⁴⁰ Regolamento Agid sulle modalità attuative, articolo 15.

⁴¹ Regolamento Agid sulle modalità attuative, articolo 16.

⁴² Regolamento Agid sulle modalità attuative, articolo 17.

Gli utenti sono obbligati a informare tempestivamente il gestore di ogni variazione degli attributi previamente comunicati. L'utente può chiedere al gestore in qualsiasi momento e a titolo gratuito la sospensione o la revoca della propria identità digitale o la modifica dei propri attributi secondari e delle proprie credenziali di accesso. Il gestore a sua volta revoca l'identità digitale se riscontra l'inattività della stessa per un periodo superiore a ventiquattro mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica. Inoltre il gestore, su richiesta dell'utente, gli segnala ogni avvenuto utilizzo delle credenziali di accesso inviandone gli estremi a uno degli attributi secondari indicati dall'utente a questo scopo.

Nel caso in cui l'utente ritenga che la propria identità digitale sia stata utilizzata abusivamente o fraudolentemente da un terzo può chiedere al gestore la sospensione immediata dell'identità digitale. Il gestore sospende tempestivamente l'identità digitale per un periodo massimo di trenta giorni, scaduto il quale l'identità digitale viene ripristinata o revocata. La revoca viene effettuata se entro trenta giorni dalla sospensione il gestore riceve dall'interessato copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione⁴³.

Per consentire all'Agid di monitorare il sistema Spid al fine di garantire l'usabilità, accessibilità e il corretto utilizzo degli elementi identificativi e indicare le migliori pratiche da adottare, i gestori devono rendere disponibili all'Agid le informazioni circa il livello di soddisfazione dei propri clienti, le caratteristiche di eventuali servizi aggiuntivi offerti e le informazioni relative a disservizi, secondo la classificazione indicata nell'articolo 30 del regolamento sulle modalità attuative.

I fornitori di servizi

Per fornitori di servizi nel contesto Spid si intendono i fornitori di servizi della società dell'informazione come definiti dalla disciplina sul commercio elettronico⁴⁴, o i fornitori dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete.

I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità digitale e ne ricevono l'esito. In base all'articolo 13 del decreto, i

⁴³ Regolamento Agid sulle modalità attuative, articolo 12.

⁴⁴ Articolo 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70. Nella nozione di servizi della società dell'informazione sono ricomprese le attività economiche svolte in linea nonché i servizi prestati normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

fornitori di servizi possono aderire allo Spid stipulando apposita convenzione con l'Agid e possono affidare la gestione delle interfacce di autenticazione informatica ai propri servizi in rete ai gestori di identità Spid.

I fornitori di servizi hanno l'obbligo di conservare per ventiquattro mesi le informazioni necessarie a imputare le operazioni effettuate sui propri sistemi alle singole identità digitali. Qualora riscontrino un uso anomalo di un'identità digitale, essi devono inoltre informare immediatamente l'Agid e il gestore dell'identità.

I dati devono essere trattati nel rispetto della disciplina sulla protezione dei dati personali; in particolare, i fornitori di servizi devono informare l'utente che l'identità digitale e gli eventuali attributi qualificati saranno verificati rispettivamente presso i gestori dell'identità digitale e i gestori degli attributi qualificati.

Per le pubbliche amministrazioni che erogano in rete servizi – direttamente o per il tramite di altri fornitori di servizi - per i quali è necessaria l'identificazione informatica dell'utente, l'articolo 14 del decreto prevede l'obbligo di consentire l'identificazione degli utenti attraverso l'uso dello Spid. A questi fini le pubbliche amministrazioni come definite dal Cad, incluse le società inserite nel conto economico consolidato della pubblica amministrazione⁴⁵, devono aderire allo Spid secondo le modalità previste dai regolamenti dell'Agenzia. Dal momento in cui è ufficializzata l'iscrizione nel registro Spid del primo gestore di identità digitale le pubbliche amministrazioni hanno ventiquattro mesi di tempo per adeguare i sistemi di log in dei propri siti all'accesso tramite Spid. Da gennaio 2016 l'Agenzia delle entrate, l'Inps, l'Inail, alcune Regioni⁴⁶ e il Comune di Firenze, che hanno partecipato alla fase di test del sistema, permettono l'accesso ai propri servizi digitali tramite Spid.

Le pubbliche amministrazioni possono affidare ai gestori di identità dello Spid le funzioni di autenticazione informatica previste dalla normativa vigente in materia nonché le funzioni di autenticazione informatica basate sugli strumenti per i quali il diritto dell'Unione europea prevede il mutuo riconoscimento. Per le pubbliche amministrazioni in qualità di fornitori di servizi è previsto l'utilizzo a titolo gratuito delle

⁴⁵Ai sensi dell'articolo 2, comma 2, del Cad, si intendono le 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, nonché alle società interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.

⁴⁶ Piemonte, Emilia Romagna, Toscana, Liguria, Marche e Friuli Venezia Giulia.

verifiche effettuate dai gestori di identità digitale e dai gestori di attributi qualificati. Per l'adeguamento allo Spid dei sistemi informatici delle amministrazioni è previsto l'utilizzo delle risorse finanziarie disponibili, senza nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 15 del decreto detta invece disposizioni che si applicano ai soggetti privati fornitori di servizi. Viene anzitutto preclusa l'adesione allo Spid nel caso di coinvolgimento in reati commessi a mezzo di sistemi informatici. In secondo luogo è previsto che per soddisfare gli specifici obblighi informativi previsti dalla disciplina sul commercio elettronico⁴⁷, i soggetti privati fornitori di servizi che aderiscono allo Spid per la verifica dell'accesso ai servizi erogati in rete, possono avvalersi della mera comunicazione del codice identificativo dell'identità digitale utilizzata dall'utente. Nella convenzione che i fornitori di servizi privati stipulano con l'Agid possono essere regolati i corrispettivi dovuti dai fornitori di servizi ai gestori di identità digitale e ai gestori degli attributi qualificati per i servizi di verifica.

3. L'Anagrafe nazionale della popolazione residente

L'Anagrafe nazionale della popolazione residente è una delle piattaforme abilitanti su cui si basa la "Strategia per la crescita digitale 2014-2020". Le piattaforme abilitanti sono strumenti chiave per promuovere lo sviluppo di servizi digitali innovativi con l'obiettivo, tra gli altri, di digitalizzare i processi e integrare le pubbliche amministrazione in un'ottica di *digital first*.

Fino ad ora la gestione dell'anagrafe della popolazione residente è stata distribuita tra le innumerevoli banche dati dei comuni la cui diversità ha comportato spesso la mancanza di interoperabilità. Questo ha spesso comportato ritardi nell'erogazione dei servizi per cui sono necessari dati demografici completi e corretti.

Il sistema dell'Anagrafe nazionale della popolazione residente è stato messo a punto per superare questa frammentazione realizzando un'unica banca dati con le

⁴⁷ In particolare, l'articolo 17, comma 2, del decreto legislativo n. 70/2003 prevede l'obbligo di informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione e dell'obbligo di fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite.

informazioni anagrafiche della popolazione residente a cui possono fare riferimento non solo i comuni ma le pubbliche amministrazioni in generale e i soggetti interessati ai dati anagrafici, tra cui in particolare i gestori dei pubblici servizi.

A dicembre 2015 è partita la fase attuativa dell'Anpr per i primi due comuni pilota; la transizione continuerà nei primi mesi del 2016 con il subentro di altri venticinque comuni pilota che hanno partecipato alla fase di sperimentazione. Il cronoprogramma prevede il completamento del processo per tutti i comuni italiani entro la fine del 2016⁴⁸.

3.1 Le disposizioni del Cad

L'Anpr è istituita ai sensi del Cad presso il Ministero dell'interno⁴⁹ e subentra all'Indice nazionale delle anagrafi⁵⁰, all'anagrafe della popolazione residente all'estero⁵¹ nonché alle anagrafi della popolazione residente e dei cittadini italiani tenute dai comuni. A questo riguardo, le disposizioni del Cad sono state recentemente modificate dal decreto legge 19 giugno 2015, n. 78, convertito dalla legge 6 agosto 2015, n. 125, che contiene disposizioni urgenti in materia di enti territoriali. In particolare tra le modifiche si prevede che l'Anpr contiene anche l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni e i dati delle liste di leva⁵².

Il regolamento anagrafico della popolazione residente, contenuto nel decreto del Presidente della Repubblica 30 maggio 1989, n. 223, è stato recentemente oggetto di modifiche e abrogazioni per essere adeguato alla disciplina istitutiva dell'Anpr. Le nuove disposizioni sono dettate dal decreto del Presidente della Repubblica n. 126 del 17 luglio 2015, in vigore dal 15 agosto 2015.

Per quanto riguarda i comuni, ai sensi dell'articolo 62 del Cad come da ultimo modificato l'Anagrafe nazionale della popolazione residente assicura la disponibilità ai singoli comuni dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi del testo unico delle leggi

⁴⁸ Cfr. <http://www.agid.gov.it>.

⁴⁹ Cad, articolo 62.

⁵⁰ L'indice nazionale delle anagrafi era istituito ai sensi dell'articolo 1, comma 5, della legge 24 dicembre 1954, n. 1228 recante l'ordinamento delle anagrafi della popolazione residente.

⁵¹ L'anagrafe della popolazione italiana residente all'estero è istituita ai sensi della legge 27 ottobre 1988, n. 470 relativa all'Anagrafe e al censimento degli italiani all'estero.

⁵² Cad, articolo 62, comma 2 bis.

sull'ordinamento degli enti locali⁵³ e mette a disposizione un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale. L'Anpr consente esclusivamente ai comuni la certificazione dei dati anagrafici⁵⁴, anche in modalità telematica. I comuni possono consentire anche mediante apposite convenzioni la fruizione dei dati anagrafici da parte dei soggetti aventi diritto.

L'Anpr assicura inoltre l'accesso ai dati in essa contenuti alle pubbliche amministrazioni e agli organismi che erogano pubblici servizi. In generale le pubbliche amministrazioni come definite dal Cad⁵⁵ si avvalgono esclusivamente dell'Anpr per la gestione e la raccolta informatizzata di dati dei cittadini, che viene integrata con gli ulteriori dati necessari per queste finalità.

3.2 Il decreto del Presidente del Consiglio dei Ministri n. 194/2014

Il decreto del Presidente del Consiglio dei Ministri n. 194 del 10 novembre 2014 prevede le modalità di attuazione e funzionamento dell'Anpr⁵⁶. In particolare esso contiene disposizioni:

- sulle modalità per attuare il graduale subentro dell'Anpr alle anagrafi comunali della popolazione residente;
- sui dati contenuti nell'Anpr e le modalità di conservazione;
- sulle garanzie e le misure di sicurezza nel trattamento dei dati personali;
- sui servizi resi disponibili dall'Anpr ai comuni e alle pubbliche amministrazioni;
- sull'accesso all'Anpr da parte dei cittadini.

Subentro alle anagrafi tenute dai comuni

Entrando nel dettaglio, è previsto che l'Anpr subentri gradualmente alle anagrafi tenute dai comuni secondo un piano e modalità idonee a garantire l'integrità, l'univocità e la

⁵³ Decreto legislativo 10 agosto 2000, n. 267, articolo 54, comma 3.

⁵⁴ La certificazione deve avvenire nel rispetto dell'articolo 33 relativo ai certificati anagrafici del decreto del Presidente della Repubblica 30 maggio 1989, n. 223.

⁵⁵ Cad, articolo 2, comma 2.

⁵⁶ Per la prima attuazione dell'Anpr è stato emanato il regolamento contenuto nel decreto del Presidente del Consiglio dei Ministri n. 109 del 23 agosto 2013.

sicurezza dei dati, descritti nell'allegato A al decreto. I dati anagrafici inviati dai comuni per il subentro sono oggetto di specifici controlli formali da parte del Ministero dell'interno.

Il Ministero dell'interno e l'Istituto nazionale di statistica, sentito il Garante per la protezione dei dati personali, definiscono standard e indicatori finalizzati a monitorare la qualità dei dati registrati nell'Anpr nella fase del subentro.

L'Anpr rende disponibile ai comuni, a seguito del subentro, i dati necessari all'allineamento delle banche dati eventualmente da questi conservate.

I dati contenuti nell'Anpr e modalità di conservazione

Nell'Anpr sono contenuti i dati del cittadino, della famiglia anagrafica e della convivenza previsti dal decreto del Presidente della Repubblica 30 maggio 1989, n. 223⁵⁷, i dati dei cittadini italiani residenti all'estero⁵⁸, nonché il domicilio digitale previsto dal Cad⁵⁹. I campi relativi ai dati sono descritti nell'allegato B al decreto.

I dati contenuti nell'Anpr sono trattati secondo le modalità e le misure di sicurezza per la protezione dei dati descritte nell'allegato C adottate nel quadro delle misure più ampie previste dalle disposizioni generali in materia di protezione dei dati personali⁶⁰. Il Ministero dell'Interno è il titolare del trattamento dei dati contenuti nell'Anpr⁶¹ e provvede alla conservazione, alla comunicazione dei dati e all'adozione delle misure di sicurezza. Il sindaco, nell'esercizio delle attribuzioni previste dal Tuel⁶², è titolare del trattamento dei dati di propria competenza limitatamente alla registrazione degli stessi.

⁵⁷ Articoli 20, 21 e 22.

⁵⁸ Si tratta dei dati registrati dai Comuni ai sensi del decreto del Presidente della Repubblica 6 settembre 1989, n. 323.

⁵⁹ Cad, articolo 3 bis.

⁶⁰ Si tratta delle misure di sicurezza, delle misure di sicurezza minima e dell'allegato B del decreto legislativo 30 giugno 2003, n. 196. Cfr. in particolare gli articoli: 31 (obblighi di sicurezza), 32 (obblighi relativi ai fornitori di servizi di comunicazione elettronica accessibili al pubblico), 32 bis (adempimenti conseguenti ad una violazione di dati personali), 33 (misure minime), 34 (trattamenti con strumenti elettronici), 35 (trattamenti senza l'ausilio di strumenti elettronici) e 36 (adeguamento).

⁶¹ Ai sensi dell'articolo 4, comma 1, lettera a), del decreto legislativo n. 196/2003, si intende per "trattamento" qualunque operazione o complesso di operazioni, effettuati senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in banca dati.

⁶² Articolo 54 del decreto legislativo n. 267/2000.

Servizi dell'Anpr disponibili per i comuni

I comuni per i quali è completato il subentro hanno accesso ai servizi dell'Anpr descritti nell'allegato D. Essi comprendono: servizi di registrazione dei dati che consentono le operazioni di modificazione dei dati di competenza del comune; servizi di consultazione che consentono di interrogare l'Anpr per i dati di competenza e servizi di estrazione che consentono di estrarre i dati dell'Anpr di propria competenza; servizi di emissione delle certificazioni anagrafiche; l'invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di morte; servizi accessori che consentono di verificare lo stato delle operazioni richieste.

Servizi dell'Anpr disponibili per le pubbliche amministrazioni e altri soggetti

Le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo n. 165/2001⁶³ e gli organismi che erogano pubblici servizi fruiscono dei servizi indicati nell'allegato D per l'espletamento dei propri compiti istituzionali. Essi comprendono: servizi di consultazione ed estrazione che consentono di interrogare i dati dell'Anpr di competenza secondo specifici parametri; comunicazione dati e variazioni anagrafiche di competenza registrate dai comuni; servizi accessori che consentono di verificare lo stato delle operazioni richieste.

L'Anpr rende disponibili all'Istituto nazionale di statistica (Istat) alcuni dati necessari alla elaborazione delle statistiche ufficiali sulla popolazione e sulla dinamica demografica.

Il Ministero dell'interno verifica i presupposti e le condizioni di legittimità dell'accesso ai servizi da parte delle pubbliche amministrazioni, dagli organismi che erogano servizi pubblici e dall'Istat.

Il comune può consentire alle pubbliche amministrazioni, anche attraverso convenzioni⁶⁴, la fruizione dei dati anagrafici della popolazione residente del proprio territorio e può consentire alle pubbliche amministrazioni e ai soggetti interessati che ne facciano richiesta per fini statistici e di ricerca, la fruizione degli elenchi degli iscritti

⁶³ Ai sensi dell'articolo 1, comma 2, del decreto legislativo n. 165/2001 per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende e amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300.

⁶⁴ Cad, articolo 62, comma 3.

all'anagrafe nazionale della popolazione residente e di dati anagrafici per fini statistici e di ricerca⁶⁵. In tutti questi casi la verifica dei presupposti e delle condizioni di legittimità dell'accesso ai dati è svolta dal sindaco.

Accesso da parte del cittadino all'Anpr

Il cittadino registrato nell'Anpr può esercitare il diritto di accesso ai propri dati personali e gli altri diritti di cui all'articolo 7 del decreto legislativo n. 196/2003 presso gli uffici anagrafici, anche consolari, o tramite il sito web dell'Anpr.

L'accesso avviene in modalità diretta e sicura, previa identificazione informatica attraverso carta d'identità elettronica, carta nazionale dei servizi o attraverso lo Spid⁶⁶, e con trasmissione dei dati in modalità protetta.

Il Direttore Generale

Micossi

⁶⁵ Articolo 34, decreto del Presidente della Repubblica n. 223/1989.

⁶⁶ Cad, articolo 64.