Camera dei deputati
Servizio Studi
XVIII Legislatura

Documentazione per l'esame di
Progetti di legge

Disposizioni concernenti la carta d'identità elettronica e la sua utilizzazione per l'accertamento dell'identità personale
A.C. 432

Dossier n° 128 - Schede di lettura
4 aprile 2019

Informazioni sugli atti di riferimento

A.C.	432
Titolo:	Disposizioni concernenti la carta d'identità elettronica e la sua utilizzazione per l'accertamento dell'identità personale
Iniziativa:	Parlamentare
Primo firmatario:	On. Fragomeli
Iter al Senato:	No
Date:	
presentazione:	28 marzo 2018
assegnazione:	26 giugno 2018
Commissione competente :	I Affari costituzionali
Sede:	referente
Pareri previsti:	II Giustizia, V Bilancio, VI Finanze, IX Trasporti, XI Lavoro, XIV Pol. Unione europea, Questioni regionali

Contenuto

La proposta di legge A.C. 432 (on. **Fragomeli** ed altri) è volta a potenziare l'utilizzo della **carta di identità elettronica (CIE**) come strumento di accertamento dell'identità del cittadino e di accesso del cittadino stesso ai servizi in rete.

In particolare, si definisce la CIE quale strumento che assicura al massimo livello di sicurezza il **riconoscimento dell'identità fisica e digitale** del cittadino e si prescrive di dotare le autorità di pubblica sicurezza degli strumenti informatici necessari per garantire l'**immediato riconoscimento della persona** (**articolo 1**).

Inoltre si prevede che la CIE diventi lo **strumento preferenziale di identificazione** di una serie di soggetti, quali:

- esercenti attività finanziaria (**articolo 2**);
- professionisti e revisori contabili (**articolo 3**);
- soggetti addetti al recupero crediti, alla custodia e al trasporto di valori, addetti alla mediazione mobiliare (**articolo 4**);
- operatori delle comunicazioni (**articolo 5**).

La proposta di legge prevede poi che anche l'**accesso a siti sensibili**, quali porti, aeroporti e stazioni ferroviarie possa avvenire tramite CIE (**articolo 6**), così come l'**accesso al luogo di lavoro** dei **dipendenti pubblici**, in sostituzione della timbratura. In quest'ultimo caso la CIE può essere utilizzata anche ai fini della verifica della effettiva presenza in servizio del lavoratore (**articolo 7**).

Infine, si stabilisce che i **servizi in rete** erogati da soggetti pubblici o privati debbano essere compatibili con i sistemi di sicurezza realizzati tramite la CIE (**articolo 8**).

La proposta di legge in esame riproduce parte delle disposizioni contenute nella pdl A.C. 4662 esaminata dalla VI Commissione Finanze della Camera nella XVII legislatura.

Riconoscimento dell'identità fisica e digitale (art. 1)

L'**articolo 1** qualifica la carta di identità elettronica quale strumento volto ad assicurare il **riconoscimento** dell'**identità fisica** e **digitale** del cittadino (**comma 1**).

La carta d'identità elettronica (CIE) rappresenta uno degli strumenti principali del processo di informatizzazione della pubblica amministrazione. Infatti, oltre a mantenere la funzione del documento cartaceo attestante l'identità della persona, la CIE dovrebbe avere la funzione di strumento di accesso ai servizi innovativi che le pubbliche amministrazioni locali e nazionali mettono a disposizione per via telematica.
La CIE è un documento amministrativo che certifica l'identità e pertanto è strettamente collegato esigenze di

pubblica sicurezza: in generale, infatti, la carta d'identità costituisce un mezzo di identificazione ai fini di polizia, ma ha carattere facoltativo e il suo ottenimento costituisce un diritto del cittadino. Tuttavia l'autorità di polizia può obbligare le persone pericolose o sospette di dotarsi della carta d'identità (art. 4, Regio decreto 18 giugno 1931, n. 773).
L'emissione della carta d'identità elettronica è riservata al Ministero dell'interno, che vi provvede nel rispetto delle norme di sicurezza in materia di carte valori, di documenti di sicurezza della Repubblica e degli standard internazionali di sicurezza (comma 2-bis dell'art. 7-vicies ter, del D.L. 43/2005 introdotto dall'articolo 10, comma 1, del decreto-legge n. 70/2011). Successivamente, l'articolo 40 del D.L. n. 1/2012 ha previsto la definizione di una tempistica graduale per il rilascio della carta d'identità elettronica. Inoltre, ha stabilito che le carte d'identità elettroniche devono essere munite anche della fotografia e delle impronte digitali della persona a cui si riferiscono.
E' affidato ad un decreto del Ministro dell'interno, di concerto con il Ministro per la pubblica amministrazione ed il Ministro dell'economia, sentita l'Agenzia per l'Italia digitale, il Garante per la protezione dei dati personali e la Conferenza Stato-città autonomie locali, la definizione delle caratteristiche tecniche, le modalità di produzione, di emissione, di rilascio della carta d'identità elettronica, nonché di tenuta del relativo archivio informatizzato. Tale decreto è stato adottato con decreto del Ministero dell'interno del 23 dicembre 2015 (vedi oltre).
Inoltre, il Ministero dell'interno può stipulare convenzioni per la gestione e il rilascio della carta d'identità elettronica con soggetti dotati di determinati requisiti, nel limite di spesa di 750 mila euro a decorrere dal 2019. Gli addetti alle procedure definite dalla convenzione sono incaricati di pubblico servizio e sono autorizzati a procedere all'identificazione degli interessati. I soggetti incaricati dalla convenzione riversano i corrispettivi delle carte d'identità elettroniche rilasciate e trattengono i diritti fissi e di segreteria (L. 145/2018, art. 1, commi 811 e 812 che hanno integrato la citata disposizione di cui all'art. 7-vicies ter, comma 2-bis del D.L. 43/2005).

L'articolo 1, **comma 2** della pdl in esame, prescrive che la carta di identità elettronica assolve ai compiti e finzioni previsti dal DPCM 24 ottobre 2014 e costituisce strumento di autenticazione al **massimo livello di sicurezza** delle identità digitali, ossia al terzo e massimo livello di sicurezza di autenticazione informatica dello SPID (DPCM 24 ottobre 2014, art. 6, comma 1, lett. c).

Il Sistema pubblico di identità digitale (SPID) è volto a consentire l'accesso a qualunque servizio con un solo pin (*Personal Identification Number*), universalmente accettato, in modo che il cittadino possa autenticarsi una sola volta presso uno dei gestori di identità digitali ed utilizzare tale autenticazione con qualunque erogatore di servizi *on line*, pubblico e privato, italiano e dell'Unione europea.
Lo SPID è stato introdotto nell'ordinamento dal decreto-legge n. 69 del 2013 (conv. dalla legge 98/2013, art. 17- ter che ha novellato l'art. 64 del CAD - codice dell'amministrazione digitale, D.Lgs. n. 82 del 2005). Con i decreti legislativi n. 179 del 2016 e n. 217/2017 – adottati entrambi in attuazione della legge di riorganizzazione della p.a. (legge n. 124 del 2015) – sono state promosse misure per favorire l'adesione da parte delle amministrazioni pubbliche e dei privati allo SPID.
Secondo quanto previsto dal CAD, l'identità digitale di un soggetto consiste nella rappresentazione informatica della corrispondenza tra esso e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale. Ai sensi dell'articolo 64 del CAD il sistema SPID è finalizzato all'identificazione degli utenti (cittadini e imprese) per consentire loro l'accesso ai servizi in rete forniti sia da parte della pubbliche amministrazioni, sia dei privati. Permane ancora la possibilità di accesso ai servizi delle p.a. anche con la carta di identità elettronica (CIE) e la carta nazionale dei servizi (CNS). Il sistema è costituito mettendo insieme i soggetti pubblici e privati (*identity provider*) che gestiscono i servizi di registrazione e di rilascio delle credenziali e degli strumenti di accesso in rete a cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.
È inoltre riconosciuta alle imprese la facoltà di avvalersi del sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete da parte dei rispettivi utenti: l'adesione esonera l'impresa dall'obbligo generale di sorveglianza delle attività sui propri siti, ai sensi del D.Lgs. n. 70 del 2003 (art. 17), che riguarda in particolare il commercio elettronico.
Con il D.P.C.M. 24 ottobre 2014 adottato su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione, di concerto con il Ministro dell'economia e sentito il Garante per la protezione dei dati personali, sono state definite le prime modalità attuative dello SPID quali:

- le caratteristiche del sistema, che comprendono il modello architetturale e organizzativo, nonché gli standard tecnologici e le soluzioni per garantire l'interoperabilità delle credenziali e degli strumenti di accesso nei riguardi di cittadini e imprese;
- le modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete, nonché quelle delle imprese in qualità di erogatori di servizi in rete;
- le modalità di accreditamento da parte dell'Agenzia per l'Italia digitale dei soggetti che gestiscono la registrazione e l'accesso in rete, c.d. gestori dell'identità digitale (comma 2-*ter*);
- i tempi e le modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete.

Il citato DPCM ha tra l'altro individuato tre livelli di sicurezza di autenticazione informatica dello SPID:

- primo livello, corrispondente al Level of Assurance LoA2 dello standard ISO/IEC DIS 29115, in cui il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a un solo fattore (ad esempio la password);
- secondo livello, corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115, in cui il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali;
- terzo livello, corrispondente al Level of Assurance LoA4 dello standard ISO/IEC DIS 29115, in cui il gestore dell'identità digitale rende disponibili sistemi di autenticazione informatica a due fattori basati su certificati digitali.

Il **comma 3** dell'articolo 1 specifica, inoltre, come realizzare il **riconoscimento dell'identità fisica** del soggetto interessato, che può essere effettuato attraverso la **lettura dei dati personali e biometrici** contenuti all'interno del **microprocessore** della carta d'identità elettronica nonché attraverso la verifica dei medesimi alla presenza del titolare della carta stessa.

A sua volta tale lettura dei dati personali e biometrici della CIE, potrà avvenire secondo le specifiche pubblicate nel Portale della stessa carta previsto dal decreto del Ministro dell'interno 23 dicembre 2015, pubblicato nella Gazzetta Ufficiale n. 302 del 30 dicembre 2015.

Ai sensi del decreto del Ministero dell'Interno del 23 dicembre 2015 (come modificato da ultimo dal D.M. 31 gennaio 2019), la carta di identità elettronica è il documento munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare.
La CIE può essere richiesta presso il proprio comune di residenza o presso il comune di dimora, o presso il consolato se cittadino italiano residente all'estero ed iscritto all'Anagrafe Nazionale della Popolazione Residente (ANPR).
Il documento può essere richiesto in qualsiasi momento e la sua durata varia secondo le fasce d'età di appartenenza. Nel dettaglio:

- 3 anni per i minori di età inferiore a 3 anni;
- 5 anni per i minori di età compresa tra i 3 e i 18 anni;
- 10 anni per i maggiorenni.

Il cittadino, nel momento della domanda:

- in caso di primo rilascio esibisce all'operatore comunale un altro documento di identità in corso di validità. Se non ne è in possesso dovrà presentarsi al comune accompagnato da due testimoni;
- in caso di rinnovo o deterioramento del vecchio documento consegna quest'ultimo all'operatore comunale;
- consegna all'operatore comunale il codice fiscale e il numero della ricevuta di pagamento della carta (se disponibile);
- verifica con l'operatore comunale i dati anagrafici rilevati dall'anagrafe comunale;
- fornisce, se lo desidera, indirizzi di contatto per essere avvisato circa la spedizione del suo documento;
- indica la modalità di ritiro del documento desiderata (consegna presso un indirizzo indicato o ritiro in comune);
- fornisce all'operatore comunale la fotografia;
- procede con l'operatore comunale all'acquisizione delle impronte digitali;
- fornisce, se lo desidera, il consenso ovvero il diniego alla donazione degli organi;
- firma il modulo di riepilogo procedendo altresì alla verifica finale sui dati.

I comuni vengono dotati di un'infrastruttura costituita da postazioni di lavoro informatiche, corredate di personal computer, stampante multifunzione, scanner di impronta, lettore per la verifica delle funzionalità del documento, lettore di codice a barre, lettore di *smart card*, attraverso le quali possono acquisire tutti i dati del cittadino, e cioè:
a) elementi biometrici primari;
b) elementi biometrici secondari;
c) firma autografa nei casi previsti;
d) autorizzazione o meno all'espatrio;
e) tramite un canale sicuro, inviarli, per la certificazione al Centro nazionale dei servizi demografici (CNSD) ubicato presso il Ministero dell'Interno, che a sua volta li trasmetterà all'IPZS per la produzione, personalizzazione, stampa e consegna del documento elettronico all'indirizzo indicato dal titolare.
Le specifiche tecniche relative al microprocessore della CIE sono contenute nel documento Carta d'Identità Elettronica. CIE 3.0 – Specifiche Chip, pubblicato sul portale www.cartaidentita.interno.gov.it.

Per garantire l'**immediato riconoscimento** della persona per accertamenti legati a questioni di pubblica sicurezza o a controlli di routine, la proposta di legge prevede che le **autorità di pubblica sicurezza** sono dotate di strumenti *hardware* e *software* e delle necessarie autorizzazioni per la verifica delle impronte digitali riportate nella carta d'identità elettronica (**comma 4**).

Ai sensi del **comma 5**, qualora sia necessario l'**accertamento dell'identità di una persona priva di documenti**, a causa di smarrimento o furto, si procede accedendo agli **schedari** tenuti dai comuni e dalle questure e confrontando i dati anagrafici e l'elemento biometrico rilevati con i dati dichiarati della persona interessata.

All'atto del rilascio o rinnovo della carta d'identità, l'ufficio comunale compila due schede: una è conservato nella segreteria del comune nell'apposito schedario, l'altro è trasmesso al questore della provincia, che ne cura la conservazione in altro schedario (regolamento di esecuzione del testo unico delle leggi di pubblica sicurezza, R.D. 635/1940, art. 290).

Verifica dell'identità ai fini dell'antiriciclaggio (artt. 2-4)

Gli **articoli 2, 3 e 4** specificano che gli **obblighi di adeguata verifica dell'identità della clientela** da parte - rispettivamente - degli **intermediari ed esercenti attività finanziaria**, dei **professionisti e dei revisori contabili**, nonché dei soggetti addetti al **recupero del credito, alla custodia e al trasporto di denaro contante, titoli o valori e alla mediazione immobiliare**, di cui al decreto legislativo 21 novembre 2007, n. 231, devono essere assolti in via preferenziale mediante lettura della **carta d'identità elettronica (CIE)**.

Come anticipato, la Carta d'identità elettronica è l'evoluzione digitale del documento di identità in versione cartacea: consente di **comprovare in modo certo l'identità del titolare**, tanto sul territorio nazionale quanto all'estero.Secondo i dati riportati nel Piano Triennale per l'informatica della Pubblica Amministrazione **2019-2021** alla data del **15/12/2018** sono state emesse **oltre 6,7 milioni di carte**; i comuni non in grado di emettere CIE sono solo 23 (su 7.915). La percentuale dei comuni in grado di emettere la CIE è pari pertanto al 99,7% dei Comuni, con una copertura del 98,7% della popolazione residente.

Si segnala che il decreto legislativo n. 231 del 2007 è stato profondamente modificato dal decreto legislativo n. 90 del 2017 in attuazione della IV direttiva antiriciclaggio (direttiva UE 2015/849). In particolare, l'articolo 1, comma 1, del decreto legislativo n. 90, ha **sostituito l'intero Titolo I** previgente.

Originariamente il Capo III del decreto legislativo n. 231 del 2007 comprendeva gli articoli da 10 a 14, che indicavano i soggetti destinatari degli obblighi. In tale ambito, gli articoli da 11 a 14 definivano, rispettivamente, le categorie degli intermediari finanziari e di altri soggetti esercenti attività finanziaria; dei professionisti; dei revisori contabili; di altri soggetti che svolgono le attività di recupero di crediti, custodia e trasporto di denaro contante e di titoli o valori, nonché di mediazione immobiliare. Con le modifiche appartate dal decreto legislativo n. 90 tali definizioni sono attualmente ricomprese nell'**articolo 3** del decreto legislativo n. 231.

L'art. 2, comma 1, del decreto legislativo n. 90 ha **sostituito** anche **l'intero Titolo II**.

Pertanto gli articoli 15, 16 e 17 del testo previgente, che si riferivano agli obblighi di adeguata verifica della clientela da parte degli intermediari finanziari e degli altri soggetti esercenti attività finanziaria, dei professionisti e dei revisori contabili, sono ricompresi all'interno dagli attuali articoli **17, 18 e 19** in materia di **disposizioni generali** degli obblighi di adeguata verifica della clientela, contenuto degli obblighi di adeguata verifica e modalità di adempimento.

Pertanto, alla luce delle modifiche introdotte dal decreto legislativo n. 90 del 2017, i testi degli articoli 2, 3 e 4 della proposta di legge in esame dovrebbe essere modificati nel senso di prevedere, in merito alla definizione dei soggetti obbligati, un unico richiamo all'articolo 3 del decreto legislativo 21 novembre 2007, n. 231 piuttosto che, rispettivamente, agli articoli 11; 12 e 13; 14.

Anche per quanto attiene agli obblighi di adeguata verifica della clientela, i testi degli articoli 2, 3 e 4 dovrebbero essere modificati nel senso di prevedere un unico richiamo agli articoli 17, 18 e 19 del decreto legislativo 21 novembre 2007, n. 231 piuttosto che, rispettivamente, agli articoli 15, 16 e 17.

Gli articoli in commento prevedono che l'adempimento degli obblighi di adeguata verifica della clientela previsti dall'articolo 17 del decreto legislativo 21 novembre 2007, n. 231, secondo le modalità indicate dagli articoli 18 e 19, ovvero **l'identificazione del cliente e la verifica della sua identità,** devono essere assolti **in via preferenziale mediante lettura della CIE.**

Si ricorda che il Capo I del D.Lgs. n. 231 del 2007 (articoli 17-30) disciplina gli obblighi di adeguata verifica della clientela: i soggetti obbligati procedono all'adeguata verifica del cliente e del titolare effettivo in occasione dell'instaurazione del rapporto continuativo o del conferimento dell'incarico per l'esecuzione professionale. La verifica deve essere effettuata, per le operazioni occasionali, non solo per le movimentazioni pari o superiori a 15.000 euro, ma anche per il trasferimento di fondi superiore a 1.000 euro. Le misure devono applicarsi sempre qualora vi sia **sospetto di riciclaggio o di finanziamento del terrorismo** ovvero **quando vi siano dubbi riguardo alla veridicità di dati precedentemente ottenuti ai fini dell'obbligo di identificazione**.

Gli articoli 18 e 19 individuano il contenuto e le modalità di adempimento degli obblighi di adeguata verifica. In particolare l'art. 18, comma 1, lett. a), prescrive **l'identificazione del cliente e la verifica della sua identità attraverso riscontro di un documento d'identità o di altro documento di riconoscimento equipollente** ai sensi della normativa vigente nonché sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. L'identificazione è estesa anche all'esecutore e deve comprendere la verifica dei poteri di rappresentanza. In presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo la verifica dell'identità può essere posticipata ad un momento successivo. In tale ipotesi di differimento, in ogni caso, occorre raccogliere i dati identificativi dei soggetti coinvolti nonché i dati relativi alla tipologia e all'importo dell'operazione. La verifica dovrà essere terminata al più presto e, comunque, entro trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico.

L'articolo 19 indica le modalità appropriate per l'identificazione, la verifica dei dati, l'acquisizione e valutazione sullo scopo e la natura del rapporto. Si prevede l'obbligatoria presenza del cliente o dell'esecutore ai fini della procedura. È richiesta l'esibizione di un documento d'identità in corso di validità o altro documento di riconoscimento equipollente ai sensi della normativa vigente, del quale viene acquisita copia in formato cartaceo o elettronico. Il cliente fornisce altresì, sotto la propria responsabilità, le informazioni necessarie a consentire l'identificazione del titolare effettivo.

I soggetti obbligati agli adempimenti in materia di lotta al riciclaggio e al finanziamento del terrorismo, tra i quali l'adeguata verifica della clientela, sono indicati all'articolo 3, in base alle funzioni effettivamente svolte: gli intermediari bancari e finanziari (comma 2); gli altri operatori finanziari (comma 3); i professionisti, nell'esercizio della professione in forma individuale, associata o societaria (comma 4); gli altri operatori non finanziari (comma 5); i prestatori di servizi di gioco (comma 6); gli intermediari bancari e finanziari e le imprese assicurative con sede legale e amministrazione in un altro Stato membro, stabiliti senza succursale sul territorio italiano (comma 6).

In particolare, **l'articolo 2** della proposta in commento dispone che gli **intermediari finanziari e gli altri**

soggetti esercenti attività finanziaria, devono assolvere l'obbligo di identificazione del cliente e la verifica della sua identità in via preferenziale mediante la lettura della carta d'identità elettronica.

L'**articolo 3** del testo in esame stabilisce anche **per i professionisti e i revisori contabili** che l'accertamento dell'identità fisica e digitale avvenga attraverso l'utilizzo della carta d'identità elettronica.

Infine, l'**articolo 4** estende anche **ai soggetti che svolgono le attività di recupero di crediti, custodia e trasporto di denaro contante e di titoli o valori e di mediazione immobiliare** la verifica in via preferenziale mediante lettura della carta d'identità elettronica dell'identità del cliente.

Operatori delle telecomunicazioni (art. 5)

L'articolo 5 prevede che gli **operatori** che sono obbligati, ai sensi del Codice delle comunicazioni elettroniche (D.Lgs. n. 259 del 2003), all'i**dentificazione dei titolari dei contratti di connettività**, debbano **garantire** la **compatibilità** di tali procedure di **identificazione e di autenticazione** per l'accesso ai servizi **con i meccanismi e i protocolli di sicurezza realizzati per il tramite della carta d'identità elettronica.**

Le specifiche saranno pubblicate nel Portale di cui al decreto del Ministro dell'interno 23 dicembre 2015, pubblicato nella *Gazzetta Ufficiale* n. 302 del 30 dicembre 2015.

Per quanto riguarda l'identificazione dei titolari dei contratti di connettività, non sono presenti nel Codice delle Comunicazioni elettroniche obblighi specifici di identificazione dei titolari, se non quelli generali derivanti dalla necessaria identificazione dei soggetti che stipulano un contratto.

Andrebbe pertanto esplicitato a quale obbligo degli operatori intenda riferirsi la disposizione, atteso che nel concetto di connettività sono ricomprese le connessioni alla rete internet.

Si ricorda in proposito che il **Codice delle Comunicazioni elettroniche,** all'articolo 40, fissa i principi generali per l'accesso e l'interconnessione, stabilendo che gli **operatori possano negoziare tra loro accordi** sulle disposizioni tecniche e commerciali relative all'accesso e all'interconnessione. L'**articolo 70,** relativo in particolare ai **diritti degli utenti finali nei contratti**, stabilisce che i consumatori ed altri utenti finali che ne facciano richiesta, hanno **diritto di stipulare contratti** con una o più imprese che forniscono servizi di **connessione ad una rete di comunicazione pubblica** o servizi di comunicazione elettronica accessibile al pubblico. Il **contratto deve indicare almeno**, in modo chiaro, dettagliato e facilmente comprensibile i seguenti elementi:

a) la denominazione e la sede dell'impresa;

b) i servizi forniti, ed in particolare:

1) se viene fornito o meno l'accesso ai servizi di emergenza e alle informazioni sulla localizzazione del chiamante e se esistono eventuali restrizioni alla fornitura di servizi di emergenza di cui all'articolo 76;

2) informazioni su eventuali altre condizioni che limitano l'accesso o l'utilizzo di servizi e applicazioni;

3) i livelli minimi di qualità del servizio offerti, compresa la data dell'allacciamento iniziale e, ove opportuno, altri parametri di qualità del servizio, quali definiti dall'Autorità;

4) informazioni sulle procedure poste in essere dall'impresa per misurare e strutturare il traffico in un collegamento di rete nel rispetto del diritto di scelta nonché del diritto alla protezione dei dati personali dell'utente onde evitare la saturazione della rete e il superamento dei limiti di capienza, e informazioni sulle eventuali ripercussioni sulla qualità del servizio riconducibili a tali procedure;

5) eventuali restrizioni imposte dal fornitore all'utilizzo delle apparecchiature terminali fornite.

c) i tipi di servizi di manutenzione offerti e i servizi di assistenza alla clientela forniti, nonché le modalità per contattare tali servizi;

d) la scelta del contraente di far includere o meno i suoi dati personali in un elenco telefonico e i dati di cui trattasi;

e) il dettaglio dei prezzi e delle tariffe, nonché le modalità secondo le quali possono essere ottenute informazioni aggiornate in merito a tutte le tariffe applicabili e a tutti i costi di manutenzione, alle modalità di pagamento e ad eventuali differenze di costo ad esse legate;

f) la durata del contratto, le condizioni di rinnovo e di cessazione dei servizi e del contratto compresi:

1) ogni utilizzo minimo o durata richiesti per beneficiare di condizioni promozionali;

2) i diritti e gli obblighi inerenti la portabilità dei numeri o di altri identificatori;

3) eventuali commissioni dovute in caso di recesso anticipato dal contratto, compresi gli eventuali costi da recuperare in relazione all'apparecchiatura terminale.

g) le disposizioni relative all'indennizzo e al rimborso applicabili qualora non sia raggiunto il livello di qualità del servizio previsto dal contratto;

h) il modo in cui possono essere avviati i procedimenti di risoluzione delle controversie ;

i) i tipi di azioni che l'impresa può adottare in risposta a incidenti o minacce alla sicurezza o all'integrità e alle vulnerabilità.

Il comma 3 dell'articolo 70 prevede che l'Autorità di regolamentazione possa richiedere che il contratto contenga ogni informazione che possa essere fornita a tal fine dalle autorità competenti sull'utilizzo delle reti e servizi di comunicazione elettronica per attività illegali e per la diffusione di contenuti dannosi, e sugli strumenti di tutela dai rischi per la sicurezza personale, la vita privata e i dati personali e relativi al servizio fornito.

Tra i principi generali del Codice, l'art. 3, comma 1, dispone infine che i provvedimenti riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, rispettino i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto dell'Unione europea. Qualunque provvedimento di questo tipo riguardante l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto

se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione deve essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto dell'Unione europea, inclusi un'efficace tutela giurisdizionale e un giusto processo.

Siti sensibili (art. 6)

L'**articolo 6** dispone che l'accesso ai porti, agli aeroporti, alle stazioni ferroviarie ed agli altri siti sensibili possa avvenire mediante accertamento dell'identità fisica secondo le modalità indicate dall'articolo 1, quindi attraverso la lettura dei dati personali e biometrici contenuti all'interno del microprocessore della carta d'identità elettronica.

Ingresso e presenza nei luoghi di lavoro (art. 7)

L'**articolo 7** concerne l'impiego della **carta d'identità elettronica ai fini della timbratura e verifica della presenza sul luogo di lavoro**.

Più nel dettaglio, si dispone che, a decorrere dai termini stabiliti con il regolamento di attuazione del provvedimento in esame (adottato con decreto del Ministro dell'interno, di concerto con gli altri Ministri interessati) presso tutti gli uffici della pubblica amministrazione la CIE sia utilizzata:

- per effettuare la timbratura in ingresso e in uscita dal luogo di lavoro (**comma 1**);
- per effettuare verifiche sull'effettiva presenza del dipendente sul luogo di lavoro, richiedendone l'utilizzo per l'accesso a postazioni di lavoro e locali (**comma 2**).

Sul punto, si ricorda che il Regolamento UE 2016/679 all'art. 4, paragrafo 1, n. 14), definisce i **dati biometrici** come quei "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".
Per questi dati, il Regolamento (art. 9) sancisce in linea generale **il divieto di trattamento,** superabile solo in presenza di alcuni presupposti tra i quali, la necessità per il titolare di adempiere a un obbligo legale o di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ovvero ancora la necessità del trattamento per l'assolvimento degli obblighi e l'esercizio dei diritti specifici (del titolare del trattamento o dell'interessato stesso) in materia di diritto del lavoro, nella misura in cui sia autorizzato "dal diritto degli Stati membri", in presenza di garanzie appropriate per i diritti fondamentali e gli interessi del soggetto passivo (art. 6, par. 1, lett. c) ed e), 3, e articolo 9, par. 2, lett. b), Reg.). Lo stesso Regolamento prevede poi una specifica riserva normativa nazionale per la disciplina dei rapporti di lavoro, consentendo a ogni Stato membro di prevedere"norme più specifiche" in materia, comprensive di "misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati" (art. 88, par. 1 e 2, Reg.). I presupposti di legittimità del trattamento dei dati biometrici, anche in materia di lavoro, attengono alla sussistenza di una previsione normativa specifica (di rango legislativo o regolamentare a seconda dei casi), alla necessità del trattamento per la realizzazione dei legittimi fini perseguiti, nonché al rispetto di garanzie appropriate. Al riguardo con il D.lgs. 108/2018 che ha modificato il Codice per la protezione dei dati personali (D.lgs n. 196 del 2003) in sede di adeguamento al Regolamento europeo, il legislatore ha previsto (con il **nuovo art. 2-septies del Codice**) un provvedimento generale del Garante recante, appunto, le **misure di garanzia necessarie per la legittimità del trattamento** dei dati genetici, **biometrici** e relativi alla salute, nell'esercizio del margine di flessibilità concesso sul punto dal legislatore europeo.

Si segnala, infine, che disposizione analoga è dettata dall'art. 2 dell'A.C. 1433 (attualmente all'esame della Camera) che prevede l'introduzione di sistemi di verifica biometrica dell'identità e anche di videosorveglianza degli accessi per i dipendenti delle amministrazioni pubbliche.

Accesso ai servizi (art. 8)

L'**articolo 8** dispone in ordine all'**accesso ai servizi in rete**, sia di quelli erogati dalle amministrazioni pubbliche centrali e locali, direttamente o tramite soggetti autorizzati, sia di quelli erogati dai privati. Quanti tra questi servizi che richiedono l'identificazione della persona interessata e la verifica della titolarità all'accesso, devono essere compatibili con i meccanismi e i protocolli di sicurezza realizzati per il tramite della carta d'identità elettronica secondo le specifiche pubblicate nel Portale di cui al decreto del Ministro dell'interno 23 dicembre 2015 (per il quale si veda l'articolo 1).

L'articolo 64 del CAD - Codice dell'amministrazione digitale prevede che l'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono l'identificazione informatica avviene tramite SPID (D.Lgs. 82/2005, art. 64, comma 2-*quater*) le cui caratteristiche sono state definite al citato DPCM 24 ottobre 2014).

Relazioni allegate o richieste

La proposta di legge, di iniziativa parlamentare, è corredata della sola relazione illustrativa.

Rispetto delle competenze legislative costituzionalmente definite

L'oggetto della proposta di legge è riconducibile alla materia *ordinamento e organizzazione amministrativa dello Stato e degli enti pubblici nazionali* rientrante nella potestà legislativa esclusiva statale ai sensi dell'art. 117, secondo comma, lett. *g),* della Costituzione.

Viene altresì in rilievo, per taluni profili, la potestà legislativa esclusiva statale nella materia della *sicurezza* ex art. 117, secondo comma, lett. g*),* Cost. e della *tutela dei mercati finanziari* (art. 117, secondo comma, lett. e*),* Cost.).

AC0227	Servizio Studi Dipartimento Istituzioni	st_istituzioni@camera.it - 066760-3855	CD_istituzioni
	Servizio Studi Dipartimento Finanze	st_finanze@camera.it - 066760-9496	CD_finanze
	Servizio Studi Dipartimento Trasporti	st_trasporti@camera.it - 066760-2614	CD_trasporti
	Servizio Studi Dipartimento Lavoro	st_lavoro@camera.it - 066760-4884	CD_lavoro