Camera dei deputati
Servizio Studi
XVII Legislatura

Documentazione per l'esame di
Progetti di legge

Impiego della carta d'identità elettronica nel contrasto del riciclaggio dei proventi di attività criminose
A.C. 4662

Dossier n° 630 - Schede di lettura
17 ottobre 2017

Informazioni sugli atti di riferimento

A.C.	4662
Titolo:	Disposizioni concernenti l'impiego della carta d'identità elettronica nell'adempimento degli obblighi di identificazione previsti dalla normativa per il contrasto del riciclaggio dei proventi di attività criminose
Iniziativa:	Parlamentare
Primo firmatario:	FRAGOMELI Gian Mario
Numero di articoli:	1
Date:	
presentazione:	27 settembre 2017
assegnazione:	4 ottobre 2017
Commissione competente :	VI Finanze
Sede:	referente
Pareri previsti:	I Affari Costituzionali, II Giustizia, V Bilancio e XIV Politiche dell'Unione Europea

Contenuto

Con la proposta di legge in esame si intende **estendere l'utilizzo della carta d'identità elettronica** nei settori dell'antiriciclaggio e all'interno del Sistema pubblico dell'identità digitale (SPID).

La **carta di identità elettronica** (CIE) è stata introdotta dalla legge n. 127 del 1997, che ha previsto la sostituzione della carta di identità cartacea con un documento realizzato su supporto informatico, contenente, oltre ai dati personali, il codice fiscale e, con l'accordo dell'interessato, l'indicazione del gruppo sanguigno. La CIE oltre a mantenere la funzione del documento cartaceo attestante l'identità della persona, ha la funzione di strumento di accesso ai servizi innovativi che le pubbliche amministrazioni locali e nazionali metteranno a disposizione per via telematica. La carta dovrà funzionare e dovrà poter essere utilizzata allo stesso modo su tutto il territorio nazionale.
Il **passaggio** verso la definizione della carta d'identità quale **carta di servizi** si ha con la modifica alla legge n. 127 operata dalla legge n. 191 del 1998, con cui viene previsto che la carta possa contenere, oltre ai dati personali, codice fiscale e gruppo sanguigno, anche altri dati che consentano l'erogazione al cittadino di quei servizi che ne richiedano l'identificazione, nonché tutte le informazioni, tra cui la chiave biometrica, necessarie per il suo utilizzo assieme alla firma digitale. Tra gli obiettivi dell'informatizzazione del documento di identità, la legge individua la possibilità del trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni.
Le disposizioni sulla carta di identità e sui documenti elettronici sono in seguito confluite nell'art. 36 del testo unico sulla documentazione amministrativa (D.P.R. n. 445 del 2000) e, successivamente, nell'**articolo 66 del Codice dell'amministrazione digitale**, che costituisce la norma di riferimento per la materia.
Nel 1999, viene approvato il regolamento che reca le regole tecniche e le modalità di rilascio (D.P.R. 22 ottobre 1999, n. 437). Con il decreto del Ministro dell'interno 19 luglio 2000 sono state dettate le regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronico.
Il quadro normativo è completato dal decreto del Ministro dell'interno 23 dicembre 2015 (recante le modalità tecniche di emissione della Carta d'identità elettronica) e dal decreto del Ministro dell'economia e delle finanze 25 maggio 2016 (recante la determinazione del corrispettivo a carico del richiedente la carta d'identità elettronica).
Da ultimo, si ricorda il decreto-legge n. 78 del 2015 (art. 10, commi 3, 4 e 5) che interviene sulla disciplina della carta di identità elettronica CIE che non è più definito quale documento obbligatorio di identificazione. Inoltre, viene definitivamente superato il progetto di unificazione della CIE e della tessera sanitaria nel Documento digitale unificato (DDU) previsto dal decreto-legge n. 70 del 2011. Il provvedimento provvede inoltre a stanziare le risorse necessarie per coprire le spese previste per l'implementazione del progetto CIE.
Secondo la pianificazione approvata dal Ministero dell'interno, entro ottobre 2017 circa 450 Comuni provvederanno ad attivare il sistema e la distribuzione della CIE ai propri cittadini, permettendo di raggiungere (insieme ai 199 comuni già in possesso del servizio di distribuzione della CIE) complessivamente il 50% della popolazione. Da ottobre 2017 è prevista la diffusione del sistema nei restanti comuni (si veda il citato Piano triennale per l'informatica nella pubblica amministrazione 2017-2019).Attualmente il servizio di rilascio è attivo in 563 comuni. Sul sito istituzionale www.cartaidentita.interno.gov.it il dato in tempo reale (al 17 ottobre 2017) riporta **982.683 carte attivate**.
Sullo stato di attuazione del progetto e sulle specifiche tecnica si veda la relazione che l'Istituto Poligrafico e Zecca

dello Stato ha presentato alla Commissione parlamentare di inchiesta istituita alla Camera sul livello di digitalizzazione e innovazione delle pubbliche amministrazioni e sugli investimenti complessivi riguardanti il settore delle tecnologie dell'informazione e della comunicazione, CIE 3.0: Overview del progetto (20 aprile 2017).

L'**articolo 1, comma 1**, della proposta in esame (A.C. 4662) prevede che gli **obblighi di identificazione prescritti dalla disciplina antiriciclaggio** (D.Lgs. n. 231 del 2007) devono essere assolti **in via preferenziale** mediante la **carta d'identità elettronica**.

Si ricorda che il **D.Lgs. n. 231 del 2007** è stato profondamente modificato dal D.Lgs. n. 90 del 2017 in attuazione della IV direttiva antiriciclaggio (direttiva UE 2015/849). La **nuova disciplina antiriciclaggio**, in particolare, aggiorna l'elenco dei soggetti destinatari degli obblighi (soggetti obbligati) e l'ambito delle prestazioni da monitorare, semplificando le modalità di conservazione dei dati e dei documenti, in applicazione del diritto europeo. Punto di partenza della direttiva è l'ampliamento e la razionalizzazione del principio dell'approccio basato sul rischio (*risk based approach*), già considerato dalla precedente direttiva, in base al quale le misure volte a prevenire o mitigare il riciclaggio e il finanziamento del terrorismo devono essere proporzionali ai rischi effettivamente individuati.
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. Gli obblighi di adeguata verifica riguardano espressamente anche i prestatori di servizi di gioco (articolo 17). 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 (richiamati dalla disposizione in commento) 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).

L'**articolo 1**, **comma 2** della pdl 4662, prescrive che, ai soli fini di identificazione della clientela da parte degli intermediari finanziari (oggetto del comma 1), la **carta di identità elettronica (CIE)** 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 il decreto legislativo n. 179 del 2016 – adottato 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, come modificato a seguito della citata legge n. 124 del 2015, 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.

Ad oggi sono disponibili solo identità SPID di primo e secondo livello (fonte: Agenzia per l'identità digitale).

Entro marzo 2018 le pubbliche amministrazioni dovranno implementare SPID in tutti i servizi digitali che richiedono autenticazione sia quelli già esistenti che quelli di nuova attivazione. L'implementazione si concluderà con la controfirma, da parte di AgID, della convenzione SPID inviata dalla PA (si veda il Piano triennale per l'informatica nella publica amministrazione 2017-2019, approvato con il DPCM 31 maggio 2017).

Il comma in esame specifica, inoltre, come effettuare 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.

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.