30 maggio 2018

Voto elettronico: pubblicazione del codice sorgente

Rapporto esplicativo concernente la modifica dell'ordinanza della CaF concernente il voto elettronico (OVE)

1 Situazione iniziale

In occasione della sua seduta del 5 aprile 2017 il Consiglio federale ha stabilito quali saranno le prossime tappe in vista dell'introduzione generalizzata del voto elettronico. L'Esecutivo si è concentrato su misure volte ad aumentare la trasparenza e sulla transizione dall'attuale fase di test a quella di operatività.

Al fine di aumentare la trasparenza, il Consiglio federale ha deciso che la pubblicazione del codice sorgente costituirà un requisito di diritto federale per l'impiego del voto elettronico, ed ha pertanto incaricato la Cancelleria federale di adeguare in tal senso l'ordinanza del 13 dicembre 2013 concernente il voto elettronico (OVE; RS *161.116*).

2 Chiesta maggior trasparenza

Con la verificabilità individuale (art. 4 OVE) e la verificabilità completa (art. 5 OVE), la Confederazione pone due condizioni in favore della trasparenza. Basata sui dati raccolti durante uno scrutinio, la verificabilità completa permette di garantire che ogni voto è stato registrato ed elaborato correttamente. I requisiti di legge per l'introduzione generalizzata del voto elettronico sono adempiti soltanto se la verificabilità completa è messa in atto e i sistemi sono stati certificati. Lo sviluppo della verificabilità completa è in corso e, se la pianificazione dei fornitori di sistemi è rispettata, dovrebbe essere concluso entro la fine del 2018.

Nel quadro dell'esame di diversi interventi parlamentari, il Consiglio federale ha più volte assicurato all'Assemblea federale che intende chiarire a fondo con i Cantoni la questione dell'accesso al codice sorgente, allo scopo di renderlo un requisito per l'autorizzazione del sistema nell'ambito della prossima revisione delle basi legali[1]. Nell'ambito del dibattito relativo alla mozione Schwaab 13.3808 «Non essere precipitosi nell'estensione del voto elettronico», è stato inoltre ribadito che Confederazione e Cantoni avrebbero valutato l'opportunità di effettuare test di intrusione pubblici. Tale valutazione si è svolta nel 2016 nel quadro del sottogruppo di lavoro «Trasparenza e pubblico». Nell'intento di aumentare la trasparenza i fornitori hanno già adottato diversi provvedimenti e pubblicato informazioni inerenti al funzionamento dei loro sistemi.

[1] Mozione 15.3492 Romano (Darbellay) «Per un sistema di voto elettronico pubblico e trasparente», mozione 15.4237 Reimann «Voto elettronico. Sì, ma solo se trasparente» e interrogazione 16.1076 Schwaab «Un test su scala reale della sicurezza del voto elettronico?».

3 Commento ai singoli articoli

Il codice sorgente è il testo di un programma informatico. È stato scritto da programmatori, è leggibile da altri programmatori e descrive il funzionamento del programma. La pubblicazione del codice sorgente va chiaramente distinta dall'attuazione della verificabilità completa. Il codice sorgente rivela *come* i voti *devono* essere registrati ed elaborati dal sistema, mentre le informazioni rilevate per la verificabilità completa permettono di stabilire *che* i voti *sono stati* registrati ed elaborati correttamente.

La pubblicazione di informazioni consente di costruire e consolidare la fiducia del pubblico. Da un lato permette agli attori specializzati di convincersi in ogni momento della sicurezza e della qualità del sistema, dall'altro conferisce alle autorità la possibilità di apportare miglioramenti in tempo utile, qualora esperti esterni dovessero constatare lacune. La pubblicazione di informazioni contribuisce infine all'oggettività del dibattito e permette di ridurre la dipendenza da singole persone e organizzazioni.

Art. 7 cpv. 2 lett. f e cpv 3 OVE

Nell'articolo 7 OVE è introdotta una distinzione concernente la verifica. La distinzione è strettamente legata alle nuove disposizioni concernenti la pubblicazione del codice sorgente previste agli articoli 7*a* e 7*b* OVE. La pubblicazione del codice sorgente deve essere effettuata *dopo* che la verificabilità completa è stata acquisita e *dopo* la certificazione. La modifica dell'articolo 7 OVE sancisce il principio secondo cui per l'impiego di un sistema completamente verificabile occorre una certificazione, indipendentemente dalla percentuale dell'elettorato ammessa. Nel caso in cui al massimo il 30 per cento dell'elettorato cantonale sia ammesso a una prova di voto, per quel che concerne il fornitore la certificazione può tuttavia limitarsi al sistema e al suo esercizio. La certificazione delle procedure cantonali, della tipografia e del software del portale dell'autorità non è invece richiesta in questo caso (cfr. in particolare i limiti di cui all'art. 7 cpv. 3 lett. b e c, OVE).

Art. 7a cpv. 1 OVE

Il codice sorgente del software del sistema deve essere pubblicato in forma facilmente leggibile. Per «software» si intende l'attuazione del protocollo crittografico per la verificabilità completa a livello applicativo. Si tratta in particolare della generazione degli elementi crittografici segreti, del controllo della validità, della registrazione dei voti entranti, del mescolamento crittografico dei voti registrati, della decodificazione dei voti e della messa a disposizione delle prove che, mediante l'impiego delle componenti di controllo, risultano dalla verificabilità completa di cui all'articolo 5 OVE.

Prima che i Cantoni presentino la domanda di autorizzazione di principio, alle persone interessate deve essere concesso sufficiente tempo per analizzare la documentazione e sottoporre le loro conclusioni alle autorità e ai fornitori dei sistemi.

Voto elettronico: pubblicazione del codice sorgente, Modifica dell'OVE

Art. 7a cpv. 2 OVE

Il codice sorgente dei sistemi deve essere pubblicato *una volta che il sistema può essere considerato completamente verificabile* e *dopo* la certificazione. Il momento della pubblicazione è determinato sulla base di quanto disposto all'articolo 7 capoversi 2 e 3 OVE. La pubblicazione può suscitare una reazione tra l'opinione pubblica (ad esempio la diffusione di notizie false [*fake news*]). Se è stato effettuato un esame preliminare credibile, le opportunità che la pubblicazione offre possono essere più importanti dei rischi insiti in tale pubblicazione.

Art. 7a cpv. 3 OVE

- Lettera a: l'impiego di componenti standard proprietari (sistemi operativi, banche dati, server web, server di applicazioni, sistemi di gestione dei diritti, firewall, router) deve essere possibile anche se il codice sorgente non è pubblicato, fermo restando che il componente sia ampiamente diffuso e quindi costantemente aggiornato. La configurazione del componente standard deve inoltre essere descritta nella documentazione relativa al sistema e al suo impiego, se ciò può contribuire a costruire una relazione di fiducia.

- Lettera b: il codice sorgente del portale di un'autorità attraverso il quale transitano i voti criptati destinati al sistema di voto elettronico non deve essere pubblicato, a condizione che le operazioni essenziali all'adempimento dell'articolo 5 OVE siano svolte nel sistema di voto elettronico.

Art. 7b cpv. 1 OVE

Questa disposizione disciplina le modalità di pubblicazione del codice sorgente. Si rinvia alle «migliori prassi», per quel che concerne ad esempio la leggibilità e la struttura del codice sorgente o le possibilità d'intervento da parte del pubblico:

- affinché possa essere letto e compreso dagli interessati, il codice deve rispettare determinati criteri legati alla leggibilità: in particolare per quanto attiene alla formattazione, ai commenti e alla complessità delle sue singole parti;

- la struttura del codice deve essere chiara; possono essere d'ausilio documentazione o illustrazioni complementari;

- la pubblicazione del codice sorgente permette al pubblico di individuarne i punti deboli: va quindi definito come gli interessati possono fornire il loro riscontro; comunicando senza indugio come saranno valutati i singoli riscontri, la fiducia nel codice sorgente potrà essere ulteriormente consolidata.

Voto elettronico: pubblicazione del codice sorgente, Modifica dell'OVE

Art. 7b cpv. 2 OVE

Nel limite del possibile, gli interessati devono poter accedere senza difficoltà al codice sorgente. Chi decide di scaricare il codice da Internet deve poterlo fare nel modo più diretto possibile. La riscossione di emolumenti è esclusa (cfr. art. 86 LDP).

Art. 7b cpv. 3 OVE

Non tutti i compiti rilevanti per la sicurezza di un sistema possono essere svolti a livello di software. Il codice sorgente non permette di determinare in che tipo di infrastruttura un sistema è gestito e quali provvedimenti di sicurezza sono adottati sotto il profilo organizzativo. Al fine di creare la trasparenza necessaria alla valutazione dell'affidabilità del sistema da parte delle cerchie interessate, il codice sorgente deve essere contestualizzato.

Art. 7b cpv. 4 OVE

I Cantoni non sono tenuti a pubblicare i software con una licenza open source, poiché i criteri corrispondenti vanno oltre la creazione di un clima di fiducia. Al fine di creare una relazione di fiducia, tuttavia, se viene utilizzato un software proprietario deve essere possibile procurarsi facilmente su Internet il codice sorgente dei programmi, analizzarlo in privato e, come avviene con i software open source, modificarlo, compilarlo ed eseguirlo in tutta legalità, nonché utilizzarlo come base per lavori scientifici. Le disposizioni sul diritto d'autore devono essere elaborate in modo corrispondente. Il proprietario del codice sorgente può autorizzarne l'impiego per altri scopi, ad esempio per l'esecuzione di uno scrutinio, o subordinarlo a condizioni.

All., n. 2.7.2

Questa disposizione vieta la conservazione dei singoli voti. La conservazione dei voti è tuttavia necessaria fino alla scadenza del termine di validazione. L'esame delle prove crittografiche risultanti dall'applicazione dell'articolo 5 OVE, ad esempio, presuppone la disponibilità delle singole schede di voto. Il numero 2.8.6 dell'allegato dell'OVE garantisce che le schede di voto precedentemente anonimizzate siano trattate in modo confidenziale.