Ordinanza della CaF concernente il voto elettronico (OVE)

del 13 dicembre 2013 (Stato 1° luglio 2018)

La Cancelleria federale svizzera (CaF),

visti gli articoli 27*c* capoverso 2, 27*e* capoverso 1, 27*f* capoverso 1, 27*g* capoverso 2, 27*i* capoverso 3 e 27*l* capoverso 3 dell'ordinanza del 24 maggio 1978[1] sui diritti politici (ODP),

ordina:

Art. 1 Oggetto e definizioni

1 La presente ordinanza fissa le condizioni per l'ammissione del voto elettronico.

2 Sono applicabili le definizioni di cui all'allegato numero 1.3.

Art. 2 Condizioni generali per l'ammissione al voto elettronico per scrutinio

L'ammissione al voto elettronico per scrutinio è rilasciata se sono adempiute le seguenti condizioni:

a. la configurazione e l'esercizio del sistema di voto elettronico (sistema) garantiscono un voto elettronico sicuro e affidabile (allegato n. 2 e 3);

b. il sistema è facile da utilizzare per gli aventi diritto di voto. Per quanto possibile sono considerate le esigenze di tutti gli aventi diritto;

c. il sistema e i processi operativi sono documentati nella misura in cui tutti i processi organizzativi e tecnici rilevanti per la sicurezza possano essere seguiti nei dettagli.

Art. 3 Analisi dei rischi

1 Mediante un'analisi dei rischi il Cantone deve documentare in maniera esauriente e comprensibile che eventuali rischi per la sicurezza sono da considerarsi sufficientemente bassi. L'analisi si riferisce ai seguenti obiettivi di sicurezza:

a. garantire la correttezza del risultato;

b. tutelare la segretezza del voto ed escludere la possibilità di stabilire in anticipo risultati parziali;

c. assicurare la disponibilità della funzionalità del voto elettronico;

RU **2013** 5371

1 RS **161.11**

d. proteggere le informazioni personali sugli aventi diritto di voto;

e. proteggere le informazioni per gli aventi diritto di voto da eventuali manipolazioni;

f. escludere la possibilità di ottenere riscontri sul comportamento di voto.

2 Ogni rischio dev'essere identificato e descritto chiaramente tenendo conto degli obiettivi di sicurezza, di eventuali serie di dati ad essi connessi, minacce, punti deboli e della documentazione relativa al sistema e al suo esercizio. Il Cantone deve motivare su questa base perché valuta i rischi come sufficientemente ridotti.

3 Per minimizzare i rischi non si possono occultare le informazioni relative alla sicurezza del sistema e del suo esercizio.

Art. 4 Requisiti per l'ammissione di più del 30 per cento dell'elettorato cantonale

1 Qualora un sistema sia ammesso per più del 30 per cento dell'elettorato cantonale, gli elettori devono avere la possibilità di constatare se il loro voto è stato manipolato sulla piattaforma utente o intercettato sulla via di trasmissione (verificabilità individuale, allegato n. 4.1 e 4.2)

2 Ai fini della verifica individuale l'elettore deve ricevere una nota di conferma secondo cui il sistema lato server ha registrato il voto, come egli lo ha immesso nella piattaforma utente, quale voto espresso conformemente al sistema. Tale nota deve confermare per ogni singolo voto la corretta registrazione.

3 Qualora i dati di autenticazione client siano inviati elettronicamente, dopo la chiusura del canale di voto elettronico gli aventi diritto di voto che non hanno votato elettronicamente devono poter richiedere, nei termini legali di ricorso, una nota di conferma secondo cui il sistema non ha registrato alcun voto che sia stato espresso utilizzando i loro dati di autenticazione client.

4 La validità di una nota di conferma non deve dipendere dall'affidabilità della piattaforma utente o dal canale di trasmissione.

5 La validità di una nota di conferma può basarsi sui seguenti elementi:

a. affidabilità del sistema lato server;

b. affidabilità di particolari ausilii tecnici degli elettori che devono adempiere requisiti di sicurezza particolarmente elevati;

c. confidenzialità di dati inviati su supporto cartaceo; la confidenzialità di questi dati dev'essere garantita al di fuori dell'infrastruttura del voto elettronico mediante particolari provvedimenti.

Art. 5 Requisiti per l'ammissione di più del 50 per cento dell'elettorato cantonale

1 Qualora un sistema sia ammesso per più del 50 per cento dell'elettorato cantonale, occorre garantire agli elettori o ai verificatori la possibilità di riconoscere, nel rispet-

to della segretezza del voto, qualsiasi manipolazione che comporti una falsificazione del risultato (verificabilità completa, allegato n. 4.3 e 4.4).

2 La verificabilità completa è data se sono adempiuti requisiti estesi in materia di verificabilità individuale (cpv. 3) e requisiti in materia di verificabilità universale (cpv. 4–6).

3 Oltre ai requisiti fissati nell'articolo 4, la verifica individuale deve adempiere i seguenti requisiti:

a. la nota di conferma deve servire agli elettori quale ulteriore conferma che i dati rilevanti per la verificabilità universale hanno raggiunto la parte affidabile del sistema (cpv. 6);

b. dopo la chiusura del canale di voto elettronico, gli elettori devono poter richiedere una nota di conferma secondo cui la parte affidabile del sistema non ha ancora registrato il loro voto che è stato espresso utilizzando i loro dati di autenticazione client;

c. la validità di una nota di conferma non deve dipendere dall'affidabilità dell'intero sistema lato server. Essa può però basarsi sull'affidabilità della parte affidabile del sistema.

4 Ai fini della verifica universale i verificatori ricevono una nota di conferma del corretto accertamento del risultato. Essi sono tenuti a valutare tale nota in un processo osservabile. A questo scopo devono avvalersi di ausilii tecnici indipendenti e isolati dal resto del sistema. La nota deve confermare che il risultato accertato considera:

a. tutti i voti espressi conformemente al sistema, registrati dalla parte affidabile del sistema;

b. solo i voti espressi conformemente al sistema;

c. tutti i voti parziali secondo la nota di conferma generata nell'ambito della verifica individuale.

5 La validità della nota di conferma può dipendere soltanto dall'affidabilità della parte affidabile del sistema e dall'ausilio tecnico impiegato per la verifica. Nel contempo la garanzia della segretezza del voto e l'esclusione di risultati parziali anticipati all'interno dell'infrastruttura del voto elettronico possono dipendere solo dall'affidabilità della parte affidabile del sistema.

6 La parte affidabile del sistema comprende un gruppo o pochi gruppi di componenti indipendenti garantite da particolari provvedimenti (componenti di controllo). Il loro impiego deve rendere riconoscibile qualsiasi abuso, qualora per ogni gruppo solo una delle componenti di controllo funzioni correttamente e in particolare sia manipolata senza che nessuno se ne accorga. Ai fini dell'affidabilità della parte affidabile del sistema la diversa configurazione delle componenti di controllo nonché l'indipendenza del loro esercizio e della loro sorveglianza è determinante.

Art. 6 Misure supplementari per minimizzare i rischi

Qualora, nonostante le misure prese, i rischi non risultino sufficientemente ridotti, occorre adottare misure supplementari per minimizzarli. Ciò vale in particolare quando tutti i requisiti previsti nell'allegato numeri 2–4 sono già stati attuati.

Art. 7 Requisiti posti alla verifica

1 I Cantoni si adoperano affinché l'adempimento delle condizioni sia verificato da organi indipendenti. La verifica ha luogo in particolare quando il sistema o il suo esercizio sono stati modificati in un modo che l'adempimento delle condizioni poste per l'ammissione potrebbe essere messo in dubbio.

2 Nel caso in cui oltre il 30 per cento dell'elettorato cantonale sia ammesso a una prova di voto (art. 4 e 5), il sistema e il suo esercizio devono essere verificati in modo particolarmente approfondito riguardo ai seguenti criteri:

a. protocollo crittografico (allegato n. 5.1);

b. funzionalità (allegato n. 5.2);

c. sicurezza dell'infrastruttura e dell'esercizio (allegato n. 5.3);

d. tutela da tentativi di introdursi nell'infrastruttura (allegato n. 5.5);

e. requisiti posti alle tipografie (allegato n. 5.6);

f.[2] impiego di un sistema che presenta la caratteristica della verificabilità completa di cui all'articolo 5: componenti di controllo (allegato n. 5.4).

3 Nel caso in cui al massimo il 30 per cento dell'elettorato cantonale sia ammesso a una prova di voto e il sistema presenta la caratteristica della verificabilità completa di cui all'articolo 5, il sistema e il suo esercizio devono essere verificati in modo particolarmente approfondito riguardo ai seguenti criteri:

a. protocollo crittografico (allegato n. 5.1);

b. funzionalità (allegato n. 5.2); la verifica può escludere i software dei portali di autorità che sono vincolati a un sistema;

c. sicurezza dell'infrastruttura e dell'esercizio (allegato n. 5.3); la verifica può vertere unicamente sull'infrastruttura che registra il voto e fornisce all'elettore la nota di conferma di cui all'articolo 4 capoverso 2;

d. tutela da tentativi di introdursi nell'infrastruttura (allegato n. 5.5);

e. componenti di controllo (allegato n. 5.4).[3]

2 Nuovo testo giusta il n. I dell'O della CaF del 30 mag. 2018, in vigore dal 1° lug. 2018 (RU **2018** 2279).

3 Introdotto dal n. I dell'O della CaF del 30 mag. 2018, in vigore dal 1° lug. 2018 (RU **2018** 2279).

Art. 7*a*[4] Pubblicazione del codice sorgente

[1] Il codice sorgente del software del sistema deve essere pubblicato.

[2] La pubblicazione avviene se il sistema presenta la caratteristica della verificabilità completa di cui all'articolo 5 dopo la verifica di cui:

a. all'articolo 7 capoverso 2, nel caso in cui oltre il 30 per cento dell'elettorato cantonale sia ammesso a una prova di voto;

b. all'articolo 7 capoverso 3, nel caso in cui al massimo il 30 per cento dell'elettorato cantonale sia ammesso a una prova di voto.

[3] Non vi è l'obbligo di pubblicare il codice sorgente di:

a. componenti terzi quali sistemi operativi, banche dati, server web e server di applicazioni, sistemi di gestione dei diritti, firewall e router, per quanto tali componenti siano ampiamente diffusi e siano costantemente aggiornati;

b. portali di autorità che sono vincolati a un sistema.

Art. 7*b*[5] Modalità della pubblicazione del codice sorgente

[1] Il codice sorgente deve essere preparato e documentato conformemente alle migliori prassi.

[2] L'accesso via Internet al codice sorgente deve essere semplice e gratuito.

[3] Una documentazione relativa al sistema e al suo esercizio deve indicare la rilevanza delle singole parti del codice sorgente per la sicurezza del voto elettronico. Tale documentazione deve essere pubblicata insieme al codice sorgente.

[4] Chiunque può esaminare, modificare, compilare ed eseguire il codice sorgente a scopi ideali nonché redigere studi in proposito e pubblicarli. Il proprietario del codice sorgente può autorizzarne l'utilizzazione ad altri fini.

Art. 8 Attestati relativi alle domande

[1] Alle domande inoltrate conformemente agli articoli 27*c* e 27*e* capoverso 1 ODP vanno allegati:

a. attestati o certificati secondo cui il sistema e il suo esercizio sono stati verificati per quanto riguarda i requisiti posti ed essi li adempiono tutti efficacemente (allegato n. 6.1–6.3);

b. attestati secondo cui, nell'imminenza di uno scrutinio, è stata effettuata un'analisi dei rischi. Detti attestati devono motivare perché i rischi valutati si muovono entro limiti sufficientemente bassi (allegato n. 6.4).

[2] È possibile rinviare ad attestati che la Cancelleria federale ha già ricevuto e che sono ancora validi.

4 Introdotto dal n. I dell'O della CaF del 30 mag. 2018, in vigore dal 1° lug. 2018 (RU **2018** 2279).

5 Introdotto dal n. I dell'O della CaF del 30 mag. 2018, in vigore dal 1° lug. 2018 (RU **2018** 2279).

Art. 9 Ulteriori disposizioni

[1] I requisiti dettagliati di natura tecnica e amministrativa posti al voto elettronico sono disciplinati nell'allegato.

[2] Sino al 30 giugno 2015 un Cantone può, in casi eccezionali, essere esonerato dall'attuazione di singoli requisiti di cui all'allegato numeri 2 e 3, sempre che:

a. l'elettorato cantonale ammesso non superi il 30 per cento;

b. i requisiti non attuati siano indicati nella domanda; e

c. il Cantone descriva le misure alternative e, per quanto riguarda l'analisi dei rischi, motivi perché esso valuta tali rischi come sufficientemente ridotti.

Art. 10 Entrata in vigore

La presente ordinanza entra in vigore il 15 gennaio 2014.

Allegato
(art. 9 cpv. 1)

Requisiti tecnici e amministrativi relativi al voto elettronico[6]

6 Il testo dell'all. alla presente O non è pubblicato nella RU (RU **2018** 2279). Può essere scaricato gratuitamente all'indirizzo www.bk.admin.ch > Temi > Diritti politici > Voto elettronico > Esigenze del diritto federale oppure ottenuto gratuitamente presso la Cancelleria federale, Sezione Diritti politici, Palazzo federale ovest, 3003 Berna.