Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF

Sezione dei diritti politici

Revisione parziale dell'ordinanza sui diritti politici e revisione totale dell'ordinanza della CaF concernente il voto elettronico (riorganizzazione della fase sperimentale)

Commento in vista dell'entrata in vigore del 1° luglio 2022

Indice

1. Situazione iniziale

In Svizzera la fase sperimentale sul voto elettronico è iniziata nel 2004. Il voto elettronico fa parte della «Strategia di e-government Svizzera» di Confederazione e Cantoni. Le basi legali per le prove di voto elettronico sono contenute nell'articolo 8*a* della legge federale sui diritti politici (LDP, RS 161.1), negli articoli 27*a*–27*q* dell'ordinanza sui diritti politici (ODP; RS 161.11) e nell'ordinanza della Cancelleria federale (CaF) concernente il voto elettronico (OVE; RS 161.116). Fin dall'inizio del progetto si è scelto di privilegiare la sicurezza, senza forzare i tempi. In Svizzera sono autorizzati soltanto i sistemi di voto elettronico che rispettano i severi requisiti di sicurezza previsti dal diritto federale.

Dal 2004 complessivamente 15 Cantoni hanno istituito le necessarie basi legali consentendo a una parte dei loro aventi diritto di voto di fruire del voto elettronico nell'ambito di oltre 300 prove svoltesi con successo. In tutti i Cantoni sono stati ammessi a partecipare alle prove gli aventi diritto di voto residenti all'estero e in alcuni Cantoni anche parte dell'elettorato residente in Svizzera. Negli ultimi anni i Cantoni avevano a disposizione due sistemi di voto elettronico: quello del Cantone di Ginevra e quello della Posta Svizzera. Tuttavia, dato che a metà 2019 entrambi i fornitori hanno ritirato il proprio sistema, attualmente in Svizzera non è più possibile votare per via elettronica.

Il 19 dicembre 2018 il Consiglio federale ha deciso di avviare la procedura di consultazione concernente il passaggio del voto elettronico all'esercizio ordinario. La revisione della LDP posta in consultazione prevedeva la conclusione della fase di sperimentazione e sanciva il voto elettronico quale terza modalità di voto ordinaria. Dalla consultazione è emerso che una chiara maggioranza dei Cantoni e dei partiti era favorevole per principio all'introduzione del voto elettronico. La Conferenza dei Governi cantonali e 19 Cantoni sostenevano il passaggio all'esercizio ordinario. Tuttavia, i partiti che si dichiaravano per principio favorevoli al voto elettronico ritenevano che fosse ancora troppo presto per compiere questo passo.

Il 26 giugno 2019 il Consiglio federale ha in seguito deciso di rinunciare per il momento alla revisione parziale della LDP. Con questa decisione ha tenuto conto anche degli sviluppi di entrambi i sistemi allora disponibili. Allo stesso tempo ha incaricato la CaF di predisporre congiuntamente con i Cantoni la riorganizzazione della fase sperimentale del voto elettronico[1]. Secondo il mandato del Consiglio federale la riorganizzazione della fase sperimentale persegue i seguenti obiettivi:

1. sviluppare ulteriormente i sistemi;
2. garantire l'efficacia dei controlli e della vigilanza;
3. rafforzare la trasparenza e la fiducia;
4. rafforzare l'interazione con il mondo scientifico.

Dopo un intenso dialogo con il mondo scientifico, Confederazione e Cantoni hanno elaborato un rapporto finale che presenta un ampio elenco di misure. Il Comitato direttivo Voto elettronico (CD VE) ha adottato tale rapporto finale sulla riorganizzazione e ripresa delle prove il 30 novembre 2020[2]. Con l'attuazione delle misure decise si intendono colmare le lacune rilevate nell'ambito dei quattro obiettivi stabiliti dal Consiglio federale. L'attuazione delle misure avverrà a tappe. Nella prima tappa è prevista l'attuazione di misure per la ripresa delle prove. Queste ultime potranno così riprendere su piccola scala, mentre si lavorerà costantemente a obiettivi a medio e lungo termine.

Nella sua seduta del 18 dicembre 2020 il Consiglio federale ha preso atto del rapporto finale del CD VE. Ha incaricato la CaF di procedere all'attuazione progressiva, da effettuarsi in collaborazione con i Cantoni, delle misure necessarie alla riorganizzazione e di presentargli un progetto da porre in consultazione comprendente i necessari adeguamenti dell'ODP e dell'OVE.

L'obiettivo del Consiglio federale è che i Cantoni possano effettuare di nuovo prove limitate di voto elettronico. La sicurezza del voto elettronico sarà garantita da norme di sicurezza più precise, prescrizioni

[1] Comunicato stampa del Consiglio federale del 27 giugno 2019; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Comunicati stampa.

[2] Il rapporto finale e i documenti concernenti il dialogo con il mondo scientifico sono consultabili sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

più severe in materia di trasparenza, una collaborazione più stretta con esperti indipendenti e una verifica efficace effettuata su mandato della Confederazione[3].

La procedura di consultazione sulla revisione parziale dell'ODP e sulla revisione totale dell'OVE nel quadro della riorganizzazione della fase sperimentale è stata aperta dal Consiglio federale il 28 aprile 2021 ed è durata fino al 18 agosto 2021. Nella consultazione hanno presentato un parere 25 Cantoni, 1 Comune, 8 partiti politici, 29 organizzazioni e diversi privati. È emerso che gli orientamenti e gli obiettivi della riorganizzazione del voto elettronico sono perlopiù accolti favorevolmente. Suscitano ampio consenso l'accento posto sull'ulteriore sviluppo dei sistemi, un controllo e una vigilanza efficaci, il rafforzamento della trasparenza e della fiducia, l'interconnessione con il mondo della scienza, ma anche il ruolo più forte della Confederazione nella verifica indipendente del sistema e del suo esercizio. Sono però state sollevate anche questioni di fondo, in particolare riguardo alle competenze di Confederazione, Cantoni e fornitori di sistema e all'obbligo di rendere pubblico il sistema di voto elettronico con una licenza *open source*. I pareri pervenuti e il rapporto sui risultati della consultazione sono stati pubblicati[4].

Nella sua seduta del 10 dicembre 2021 il Consiglio federale ha preso atto del risultato della procedura di consultazione e ha incaricato la CaF di completare le ordinanze tenendo conto delle dettagliate osservazioni sulle singole disposizioni, in modo tale che i Cantoni possano riprendere le prove di voto[5]. Le riserve su aspetti di fondo espresse nella consultazione vanno considerate a medio e a lungo termine nel senso dell'elenco di misure di Confederazione e Cantoni secondo il rapporto finale del CD VE del 30 novembre 2020.

2. Panoramica della revisione delle basi legali 2022

La revisione delle basi legali comprende una revisione parziale dell'ODP e una revisione totale dell'OVE e del suo allegato, che entreranno in vigore il 1° luglio 2022. Queste modifiche portano a compimento la prima tappa dell'attuazione delle misure sulla riorganizzazione della fase sperimentale.

Qui di seguito sono illustrati gli aspetti salienti della revisione.

- **Proseguimento della fase sperimentale**
  Il voto elettronico proseguirà nella fase sperimentale. Finora le disposizioni federali prevedevano tre livelli nella limitazione dell'elettorato a seconda del grado di sviluppo dei sistemi. Nella prossima tappa della sperimentazione il limite è fissato anche per l'impiego di sistemi completamente verificabili in modo unitario al 30 per cento al massimo dell'elettorato cantonale e al 10 per cento al massimo dell'elettorato svizzero. I limiti sono periodicamente riesaminati sulla base degli sviluppi nel settore del voto elettronico. Come finora, gli Svizzeri all'estero aventi diritto di voto non sono considerati nel calcolo dei limiti (art. 27*f* cpv. 3 ODP). Con la nuova normativa anche gli aventi diritto di voto con disabilità che non possono esprimere il loro voto autonomamente nel rispetto del segreto del voto saranno esclusi dal conteggio dei limiti.

- **Sicurezza rafforzata**
  In futuro la Confederazione autorizzerà soltanto sistemi completamente verificabili. È questa una misura importante per garantire la sicurezza del voto elettronico: la verificabilità completa consente di rilevare manipolazioni dei voti espressi per via elettronica. La sicurezza del sistema di voto elettronico deve essere ulteriormente rafforzata con precise direttive in materia di sicurezza e qualità per i sistemi e il loro sviluppo.

- **Ripartizione delle competenze tra Confederazione e Cantoni**
  Come ora, ogni Cantone deciderà da sé se effettuare prove di voto elettronico. Anche l'acquisizione del sistema resta di competenza dei Cantoni: come ora possono gestire un proprio sistema, utilizzare

[3] Comunicato stampa del Consiglio federale del 21 dicembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Comunicati stampa.

[4] Consultabili sotto www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2021 > CaF.

[5] Comunicato stampa del Consiglio federale del 10 dicembre 2021; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Comunicati stampa.

il sistema di un altro Cantone oppure far capo al sistema di un'impresa privata (art. 27*k*^{bis} lett. b ODP). La Confederazione stabilisce, come finora, il quadro normativo ed è responsabile per la concessione delle autorizzazioni.

- **Verifiche indipendenti**
  Al posto di porre l'accento, come finora, sulla certificazione dei sistemi e dell'esercizio, una verifica indipendente su mandato della Confederazione consentirà un esame della sicurezza e, in tal modo, dell'adempimento dei requisiti per l'autorizzazione, nonché di rilevare un potenziale di miglioramento per il futuro. Con la presente revisione, per la parte principale degli esami sarà la Cancelleria federale e non i Cantoni o il gestore del sistema a conferire il mandato.

- **Trasparenza, coinvolgimento del pubblico e collaborazione con il mondo scientifico**
  Disposizioni volte a rafforzare la trasparenza e il maggiore coinvolgimento di specialisti indipendenti nella concezione, sviluppo ed esame di sistemi di voto elettronico devono contribuire a instaurare un processo di costante perfezionamento. Il pubblico avrà accesso a tutte le informazioni concernenti il sistema, l'esercizio e i rapporti d'esame e sarà promossa la partecipazione. In tal modo si pongono solide basi per una verifica pubblica permanente, per la quale un ruolo importante è anche svolto dal mondo scientifico. In quest'ambito gli attuali requisiti concernenti la pubblicazione del codice sorgente del sistema di voto elettronico saranno precisati e si sancirà l'obbligo di effettuare un programma *bug bounty*. Questo programma prevedrà un'indennizzazione finanziaria per le segnalazioni di rilievo giunte dal pubblico.

3. Ripercussioni per la Confederazione, i Cantoni e altri attori

Per esprimere il voto elettronicamente la sicurezza è fondamentale. Questa esigenza ha notevoli ricadute finanziarie per le autorità e i fornitori dei sistemi. I costi sono imputati secondo la ripartizione delle competenze tra Confederazione e Cantoni nel settore dei diritti politici: la parte preponderante dei costi sarà ancora a carico dei Cantoni.

È stato stimato che l'attuazione della prima tappa delle misure previste nel periodo 2021–2022 comporterà per i Cantoni costi supplementari di 1,2–1,5 milioni di franchi. I costi annuali d'esercizio supplementari ammonteranno verosimilmente a circa 50 000–70 000 franchi. Per l'attuazione delle misure sul medio e lungo termine si prevedono ulteriori costi tra 3,4 e 4,1 milioni di franchi. Queste misure comportano un aumento dei costi d'esercizio annuali tra 0,9 e 1,1 milioni di franchi. Queste stime comprendono i costi totali per tutti i Cantoni.

La Confederazione stima per la prima tappa, prevista nel periodo 2021–2022, costi supplementari *una tantum* pari a 1,25 milioni di franchi, che comprendono in particolare le verifiche indipendenti dei sistemi di voto elettronico che dovranno in futuro essere commissionate dalla CaF. Sul medio e lungo termine occorre mettere in conto costi ricorrenti. La riorganizzazione della fase sperimentale non ha alcuna ricaduta sull'organico di personale della Confederazione.

I costi saranno verosimilmente sopportati per un lungo periodo di tempo da pochi Cantoni. Se l'introduzione del voto elettronico sarà garantita sul lungo periodo, la Confederazione dovrà partecipare nella fase sperimentale in modo più importante ai costi dei Cantoni. Il Consiglio federale ritiene pertanto opportuno che la Confederazione partecipi finanziariamente ai costi di sviluppo e si impegna affinché possa farlo attraverso l'Amministrazione digitale Svizzera (ADS). Nel quadro del Piano di attuazione 2021-2023 l'ADS ha accolto una prima proposta di finanziamento del fabbisogno supplementare di fondi.

Le misure per la riorganizzazione si ripercuotono inoltre sulla Posta Svizzera, che al momento è l'unico fornitore di sistema. La Confederazione non è a conoscenza di eventuali costi a carico della Posta che superino le summenzionate stime dei costi concernenti Confederazione e Cantoni.

4. Commento alle singole disposizioni

4.1 Ordinanza sui diritti politici (ODP)

La revisione parziale dell'ODP comprende in particolare le modifiche per l'attuazione della riorganizzazione della fase sperimentale del voto elettronico (modifiche nella sezione 6*a*: Prove del voto elettronico, cfr. n. 4.1.1). Prevede inoltre alcuni aggiornamenti nella sezione 3 e nell'allegato 3a dell'ODP (cfr. n. 4.1.2).

4.1.1 Adeguamenti nella sezione 6*a*: Prove del voto elettronico

Art. 27b lett. b

Per le prove di voto è prevista una procedura di autorizzazione a due fasi: i Cantoni necessitano di un'autorizzazione di principio del Consiglio federale che è accordata per più scrutini o per le elezioni del Consiglio nazionale (art. 27*a* ODP); in aggiunta per ogni scrutinio è necessario un nulla osta della CaF (art. 27*e* ODP). Il Consiglio federale può accordare un'autorizzazione di principio soltanto se le condizioni per la concessione del nulla osta stabilite nell'OVE sono adempiute. La CaF esamina nell'ambito della procedura per il nulla osta se tali condizioni sono adempiute. La procedura per l'autorizzazione di principio comprende pertanto sempre anche la procedura di concessione del nulla osta. Per chiarire questo rapporto tra l'autorizzazione di principio e la procedura per il nulla osta, la lettera b è integrata con un rinvio all'adempimento delle condizioni per la concessione del nulla osta. Questa modifica costituisce semplicemente una precisazione del disciplinamento vigente e, in tal modo, corrisponde all'attuale prassi e non ha alcuna conseguenza pratica sulla procedura per il rilascio dell'autorizzazione di principio e della concessione del nulla osta.

Art. 27c cpv. 2

Con l'adeguamento dell'articolo 27*b* lettera b ODP questa disposizione può essere abrogata.

Art. 27d lett. c

Nell'autorizzazione di principio il Consiglio federale, oltre che per quale territorio, stabilisce per quale percentuale dell'elettorato – ovvero quale quota di aventi diritto di voto – è autorizzato il voto elettronico. Il Consiglio federale necessita dell'indicazione del numero di aventi diritto di voto che devono essere ammessi al voto elettronico per verificare il rispetto dei limiti secondo l'articolo 27*f* capoverso 1 ODP.

Art. 27e cpv. 1–2

Come nella fase sperimentale finora svolta, per ogni scrutinio è richiesto un nulla osta da parte della CaF. Poiché il Consiglio federale accorda un'autorizzazione di principio per più prove di voto (ad eccezione delle elezioni del Consiglio nazionale), a livello di CaF si esamina per ciascuna prova se le condizioni sono (ancora) adempiute. Le condizioni per il nulla osta sono definite nell'OVE.

Cpv. 1 e 1bis: questi capoversi riprendono il precedente capoverso 1 con l'integrazione che la CaF stabilisce i requisiti che il sistema e il suo esercizio devono soddisfare. La delega finora presente nell'articolo 27*f* ODP è ora disciplinata in questa sede.

Cpv. 2: revisione redazionale.

Art. 27f Limiti

Cpv. 1: la graduazione secondo limiti finora prevista era vincolata all'attuazione dei requisiti di sicurezza. Per i sistemi con verificabilità completa il Consiglio federale avrebbe potuto autorizzare un impiego senza limiti. Nella fase sperimentale finora condotta nessun Cantone ha adempiuto le condizioni per ammettere

più del 30 per cento dell'elettorato cantonale al voto elettronico. Anche il limite del 10 per cento dell'elettorato svizzero non è finora mai stato raggiunto[6]. È ora previsto di fissare anche per l'impiego di sistemi completamente verificabili un limite unitario al 30 per cento dell'elettorato cantonale e al 10 per cento dell'elettorato svizzero. Con questa limitazione unica alla categoria finora più bassa si intende sottolineare il carattere sperimentale del voto elettronico.

Come finora, il rispetto dei limiti cantonali è di competenza dei Cantoni. Essi possono stabilire liberamente come assicurare il rispetto dei limiti per gli aventi diritto di voto residenti nel Paese. Nella prassi erano finora ad esempio previsti una procedura di iscrizione oppure il ricorso a Comuni pilota.

Per il rispetto dei limiti nell'impiego a livello nazionale è responsabile la Confederazione. Se, a causa dei limiti nazionali, non è possibile rilasciare un'autorizzazione di principio a tutti i Cantoni che ne fanno richiesta, la priorità è data al rilascio delle autorizzazioni di principio periodiche rispetto alle nuove autorizzazioni di principio. In tal modo si dà la precedenza alla continuità del voto elettronico nei Cantoni che già l'hanno impiegato e che fanno richiesta di una nuova autorizzazione di principio, rispetto ai Cantoni che vogliono iniziare a sperimentare questa modalità di voto.

Cpv. 2: la limitazione di cui al capoverso 1 sarà applicabile nella prossima fase sperimentale. I Cantoni devono avere la possibilità di acquisire esperienza con l'impiego di sistemi completamente verificabili, mentre le sperimentazioni rimangono limitate. Con un riesame periodico dei limiti è possibile tenere conto degli sviluppi nel voto elettronico. Si tratta di valutare l'impiego attuale e previsto del voto elettronico nei Cantoni, il contesto politico, la stabilità dell'esercizio sperimentale e la fiducia riposta dalla popolazione nel voto elettronico. La CaF può avviare una tale valutazione da sé o su sollecitazione dei Cantoni. Se sulla base di questi elementi riterrà opportuno un adeguamento dei limiti, la CaF presenterà al Consiglio federale una relativa proposta per modificare il capoverso 1.

Cpv. 3: ex capoverso 2 con la seguente modifica: oltre agli Svizzeri all'estero aventi diritto di voto, tra i gruppi destinatari particolari del voto elettronico figurano anche gli aventi diritto di voto che a causa della loro disabilità non possono esprimere il proprio voto autonomamente. Con l'integrazione del capoverso 3 questi due gruppi di aventi diritto di voto possono essere esclusi dal conteggio per i limiti. In tal modo i Cantoni hanno la possibilità di offrire il voto elettronico a questi due gruppi indipendentemente dalle disposizioni concernenti le limitazioni dell'elettorato. L'attuazione delle eccezioni spetta ai Cantoni. Per l'impostazione e l'applicazione delle disposizioni concernenti le persone disabili, i Cantoni devono possibilmente coinvolgere specialisti in materia di politica dei disabili e accessibilità senza barriere.

Art. 27i, rubrica, nonché cpv. 1 e 2 Verificabilità e controllo della plausibilità del voto elettronico

L'affidabilità del voto elettronico è pretesa dall'articolo 27*j* ODP. L'articolo 27*i* ODP disciplina la tracciabilità come verificabilità del corretto trattamento dei voti, della correttezza del risultato e del controllo della plausibilità del voto. La formulazione dell'articolo 27*i* capoversi 1 e 2 si riferisce alla possibilità di autorizzare al voto elettronico soltanto una parte o l'intero elettorato. Poiché secondo l'articolo 27*f* capoverso 1 ODP nella prossima fase sperimentale non è prevista la possibilità di autorizzare l'intero elettorato, occorre modificare la formulazione. Inoltre, i due capoversi sono stati invertiti e la rubrica è stata adeguata di conseguenza per anteporre la verificabilità al controllo della plausibilità.

Cpv. 1: La verificabilità del voto elettronico è la misura centrale per garantire la sicurezza del voto elettronico perché consente di rilevare manipolazioni dei voti espressi elettronicamente. La verificabilità prevede che si controlli o si possa controllare se un voto:

- è stato espresso conformemente all'intenzione del votante;
- è stato registrato nel modo in cui è stato espresso;
- è stato conteggiato nel modo in cui è stato registrato.

Nel disciplinamento vigente è richiesta la verificabilità completa se l'intero elettorato è coinvolto nella prova di voto. D'ora in poi la verificabilità completa sarà richiesta indipendentemente dalla quota dell'elettorato ammesso al voto.

[6] La quota più alta si è registrata nella votazione del 10 febbraio 2019: il 2,5 per cento degli aventi diritto di voto residenti in Svizzera è stato ammesso al voto elettronico.

Cpv. 2: la plausibilità dei risultati del voto elettronico deve fornire indicazioni su eventuali errori nella trasmissione dei dati e su possibili manipolazioni dei risultati. Come finora, i Cantoni possono controllare la plausibilità mediante diversi metodi. Ad esempio, possono confrontare i risultati con quelli del voto per corrispondenza o del voto di persona all'urna, paragonare i voti elettronici scrutinati e i file di registro (file di log) del server della votazione o dell'elezione o verificarli sulla base di voti di controllo espressi ad esempio dalla rappresentanza degli aventi diritti di voto. Nelle sperimentazioni si devono utilizzare – se disponibili e se la base dei dati lo consente – metodi statistici. La Confederazione e i Cantoni si sono accordati nell'ambito del rapporto finale del CD VE per sviluppare ulteriormente il controllo della plausibilità dei risultati[7].

I capoversi 3 e 4 restano immutati.

Art. 27k^{bis} cpv. 2

La disposizione può essere abrogata, perché a differenza dalla prassi vigente la CaF non è più coinvolta nelle relazioni contrattuali. Il rapporto contrattuale tra i Cantoni ed eventuali imprese private si desume dal capoverso 1.

Art. 27l Verifica dei sistemi e delle modalità d'esercizio

Cpv. 1: riprende la precedente disposizione del capoverso 2 e disciplina quando è necessaria una verifica. Cfr. a tal proposito anche le disposizioni sul momento della verifica al numero 26 dell'allegato dell'OVE.

Cpv. 2: gli oggetti della verifica corrispondono sostanzialmente al disciplinamento vigente. La precedente nozione di «requisito in materia di sicurezza» è ampliata a tutti i requisiti della CaF, ciò che corrisponde nel contenuto all'attuale applicazione. Inoltre, l'ente esaminatore deve essere indipendente dall'ente esaminato.

Cpv. 3 e 4: la CaF disciplina nella sua ordinanza i contenuti da esaminare, le scadenze delle verifiche, i requisiti posti agli enti incaricati, nonché chi è competente a commissionare il mandato. Dalla revisione delle basi legali nel 2013, nella maggior parte delle volte la verifica dei sistemi di voto elettronico è stata commissionata a enti esterni accreditati. Spettava ai Cantoni commissionare da sé o attraverso il gestore del sistema la certificazione richiesta. Le esperienze del 2019 hanno dimostrato che le attuali esigenze poste nell'ambito delle verifiche dei sistemi e dei processi si sono rivelate di scarsa efficacia. In seguito alla pubblicazione del codice sorgente e a una successiva verifica indipendente sono state individuate lacune considerevoli in materia di sicurezza, che non erano state constatate durante i controlli e le certificazioni. Per garantire l'efficacia e la credibilità della verifica, si adeguano le competenze e le verifiche dei sistemi[8]. Nell'adeguare le competenze occorre prestare grande importanza all'indipendenza fra l'ente incaricato della verifica e l'ente oggetto della verifica. La suddivisione dei compiti fra la Confederazione e i Cantoni viene quindi modificata in modo tale che la Confederazione assuma maggiori responsabilità e un ruolo più diretto nella verifica dei sistemi.

Art. 27l^{bis} Pubblicità delle informazioni sul sistema e il suo esercizio

Cpv. 1: la pubblicazione di informazioni sul sistema di voto elettronico e sul suo esercizio serve a verificare il corretto svolgimento del processo. I destinatari sono sia gli specialisti sia persone senza conoscenze specialistiche.

Cpv. 2: la misura principale in questo contesto è la pubblicazione del codice sorgente e della relativa documentazione (lett. a e b). Conformemente agli articoli 7*a* e 7*b* OVE, i Cantoni sono già tenuti secondo le vigenti basi legali a pubblicare il codice sorgente del software di un sistema di voto elettronico completamente verificabile, unitamente a una documentazione sufficiente. Il codice sorgente permette di vedere

[7] Cfr. la misura B.8 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

[8] Cfr. la misura B.1 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

in che modo il sistema deve registrare ed elaborare i voti. La lettera c prevede che sia resa pubblica anche la documentazione del processo di sviluppo. Per processo di sviluppo s'intende qui l'intero processo per la realizzazione del codice sorgente e i suoi meccanismi di controllo e approntamento. I requisiti posti al processo di sviluppo sono stabiliti ai numeri 24.1 e 24.3–24.5 dell'allegato dell'OVE. Comprendono in particolare il ciclo di vita, gli strumenti di sviluppo, i metodi di sviluppo, la gestione delle modifiche, la gestione della configurazione, la compilazione e il *deployment* affidabili e verificabili. Non comprendono tuttavia i prodotti derivanti da questi processi (come *change request*, elenchi di configurazione o la *commit history)*. Secondo la lettera d è ora resa pubblica una prova che confermi che il codice sorgente pubblicato sia anche quello attuato nell'impiego del sistema.

I principi della trasparenza e della comprensibilità sono importanti e devono essere sanciti nell'ODP. Le informazioni pubblicate consentono alle cerchie di specialisti di partecipare al processo, a tutto vantaggio della sicurezza, della qualità del sistema e della fiducia. La pubblicazione di informazioni relative al sistema, in particolare al codice sorgente, e al suo esercizio consente un dibattito obiettivo e basato sui fatti. La disponibilità delle informazioni favorisce l'indipendenza da singole persone e organizzazioni. La CaF continuerà ad apportare le precisazioni necessarie nella sua ordinanza.

Cpv. 3: in casi motivati è possibile rinunciare alla pubblicazione. Se alla pubblicazione si oppongono interessi pubblici o privati preponderanti, si deve valutare se non sia possibile una forma di pubblicazione alternativa (p. es. annerimento di determinati passaggi o descrizione riassuntiva dei contenuti). Se non è possibile alcuna forma di pubblicazione alternativa che assicuri la tutela degli interessi preponderanti, in tal caso, e soltanto in tal caso, si deve rinunciare alla pubblicazione. Per stabilire gli interessi preponderanti ci si orienta in linea di massima agli interessi che danno luogo a eccezioni secondo la legislazione in materia di trasparenza e di protezione dei dati. Si tratta di ponderare di volta in volta tra l'interesse pubblico a una pubblicazione e l'interesse pubblico o privato alla confidenzialità. Occorre partire dal principio che l'interesse pubblico alla trasparenza, per quanto riguarda argomenti rilevanti per la sicurezza, è elevato. Quali interessi alla confidenzialità è possibile far valere direttive interne, la protezione di informazioni interne di un'impresa o la protezione dei dati di terzi.

Art. 27l^{ter} Coinvolgimento del pubblico

Cpv. 1: per coinvolgere il pubblico e soprattutto le cerchie di specialisti la CaF e i Cantoni attuano misure come l'organizzazione di convegni scientifici e conferenze, di concorsi di idee e *hackathon*, la gestione di piattaforme informative o l'attuazione di progetti di *citizen science*. Inoltre, la CaF si incarica qui, tra l'altro, di spiegare la nozione di verificabilità. I Cantoni sono responsabili di spiegare l'attuazione della verificabilità conformemente all'articolo 27*m* capoverso 1.

Cpv. 2: i Cantoni sono in particolare incaricati di predisporre gli incentivi per coinvolgere specialisti del pubblico al fine di migliorare i sistemi di voto elettronico, ad esempio con l'attuazione di programmi di *bug bounty* da parte dei Cantoni (art. 13 OVE).

Art. 27m Informazione degli aventi diritto di voto e pubblicazione dei risultati del voto elettronico

Cpv. 1: questo capoverso è stato modificato leggermente sotto il profilo redazionale. Come finora i Cantoni dovranno informare gli aventi diritto di voto. Si tratta in particolare di informazioni che figurano sul materiale di voto, ovvero indicazioni concrete su come funziona il voto elettronico e come comportarsi in caso di irregolarità o problemi. Inoltre, si ritiene importante informare gli aventi diritto di voto sull'attuazione della verificabilità. In effetti, la procedura della verificabilità permette di rilevare eventuali irregolarità solo se essa è utilizzata anche dagli elettori. La verificabilità completa consente di promuovere la fiducia soltanto se si riesce a coglierne l'utilità.

Cpv. 2: corrisponde nei principi al precedente capoverso 2. La disposizione è stata precisata chiarendo che ci si riferisce alla possibilità di osservare gli atti nello svolgimento di uno scrutinio (p. es. la procedura di spoglio, il crittaggio e la decrittazione dell'urna elettronica). Questa disposizione contribuisce ulteriormente alla trasparenza nei confronti degli aventi diritto di voto. Come finora, la disposizione non esige che i Cantoni attuino strutture permanenti destinate a rappresentare gli elettori, ad esempio commissioni elettorali. In linea generale è sufficiente che le procedure e i processi possano essere seguiti ad esempio

da un ufficio elettorale, istituito dall'autorità competente, poiché questo è generalmente composto di persone con diritto di voto nel Cantone. Del resto, non si tratta né di rendere accessibili *tutte* le tappe né di pubblicare *tutti* i documenti. Se vi sono fondati motivi che ne sconsigliano l'accesso o la pubblicazione, rimane sempre la possibilità – come è stato il caso finora – di respingere la domanda. A tale riguardo è possibile rifarsi alle eccezioni previste nella legislazione applicabile in materia di trasparenza. Il rimando alla legge federale del 17 dicembre 2004 sul principio di trasparenza dell'amministrazione non è più considerato necessario e può pertanto essere stralciato. È determinante che lo scrutinio avvenga in tempo utile: in nessun momento il buon svolgimento dello scrutinio deve essere messo in pericolo da questa disposizione.

Cpv. 3: i Cantoni sono ora obbligati a pubblicare i risultati dei voti espressi per via elettronica. La pubblicazione serve in primo luogo per assicurare la trasparenza.

Devono essere pubblicati i seguenti risultati:

- nelle votazioni: il numero di voti espressi per via elettronica con un Sì, un No o in bianco;
- nelle elezioni: il numero di voti espressi per via elettronica per candidato (voti personali) e per lista (voti di lista).

In linea di massima i dati devono essere pubblicati in modo dettagliato. Nelle votazioni si deve prevedere la pubblicazione dei dati per Comune e nelle elezioni dei dati per circondario elettorale. Il segreto del voto non deve essere compromesso dalla pubblicazione dei risultati. Il segreto del voto è per esempio compromesso se sono autorizzati al voto elettronico soltanto gli Svizzeri all'estero e in un Comune vi è un'unica persona in vita residente all'estero che ha diritto di voto. Se la pubblicazione rischia di pregiudicare il segreto del voto, piuttosto che derogare al principio della pubblicazione dei risultati si devono di norma esaminare vie alternative. Occorre ad esempio valutare se e in che modo procedere a una pubblicazione con un grado di dettaglio dei risultati modificato, come il riassunto dei risultati di più Comuni. Si rinuncia alla pubblicazione se non vi è alcuna forma di comunicazione alternativa che consenta di garantire il segreto del voto.

Non è necessario pubblicare i risultati sul Foglio ufficiale, ma è sufficiente presentarli sul sito Internet del Cantone. Le informazioni devono essere facilmente accessibili e riutilizzabili.

Art. 27o Ricorso a specialisti indipendenti e accompagnamento scientifico

Cpv. 1: nei loro lavori le autorità devono essere maggiormente seguite, laddove la loro presenza è utile, da specialisti indipendenti, ad esempio quando si possono ricavare conoscenze su questioni concernenti la sicurezza del voto elettronico. Gli specialisti dovrebbero essere indipendenti dai gestori del sistema e, se possibile, anche dalle autorità. Potrebbero entrare in linea di conto mandati a specialisti per prestazioni concrete o consulenze, come la verifica del sistema, il sostegno o la consulenza nell'elaborazione di analisi dei rischi, la verifica e la consulenza relativi alla facilità d'uso e all'accessibilità senza barriere del sistema, oppure la collaborazione nell'esercizio, ad esempio nella valutazione di risultati di verifica e in eventuali indagini successive.

Cpv. 2: la CaF deve inoltre provvedere affinché le prove di voto elettronico siano accompagnate sotto il profilo scientifico. Questa disposizione comprende lavori di ricerca da parte delle cerchie scientifiche che – a differenza del capoverso 1 – non devono servire direttamente ai lavori delle autorità indispensabili per tenere gli scrutini. Questo accompagnamento scientifico deve favorire la creazione di una base che serva alla valutazione e a indicare in che modo perfezionare la fase sperimentale. Le lettere a e b possono tra l'altro comprendere lavori di ricerca sui temi seguenti:

- Requisiti per la fiducia e l'accettazione
- Utilizzazione del voto elettronico
- Rafforzamento della verificabilità
- Metodi formali per la formulazione delle esigenze e delle specifiche del sistema
- Facilità d'uso e accessibilità senza barriere

Cpv. 3: corrisponde sostanzialmente al precedente capoverso 2.

Cpv. 4: corrisponde al precedente capoverso 3.

4.1.2 Adeguamenti nella sezione 3 e nell'allegato 3*a*

Art. 8a cpv. 1

Questa disposizione è stata rimaneggiata sotto il profilo redazionale. Dal 1° novembre 2015 i Cantoni con il sistema proporzionale devono designare come termine per la presentazione delle proposte di candidatura un lunedì nel mese di agosto dell'anno delle elezioni (RU **2015** 543). Nei Cantoni con il sistema maggioritario e che prevedono la presentazione delle candidature, in futuro sarebbe tuttavia anche ipotizzabile, a seconda delle circostanze, un termine di presentazione per inizio settembre.

Art. 8d cpv. 3

Nella prassi per questa notifica non si utilizza più il telefax. La diposizione può pertanto essere corretta di conseguenza.

Allegato 3a e allegato 3a retro

Si procede a diversi adeguamenti a seguito della modifica del 26 settembre 2014 della LDP (RU **2015** 543).

4.2 Ordinanza della CaF concernente il voto elettronico (OVE)

4.2.1 Parte principale

Art. 1 Oggetto

Le definizioni sono ora dislocate nella parte principale dell'OVE (cfr. art. 2 OVE).

Art. 2 Definizioni

Cpv. 1: riprende essenzialmente le definizioni della versione vigente dell'allegato dell'OVE, nella misura in cui sono rilevanti per la parte principale.

Spiegazioni concernenti le singole definizioni:

Lett. a: rientrano nello «svolgimento di scrutini per via elettronica» anche i preparativi e i lavori successivi, sempre che queste attività concernano specificamente il voto elettronico. Non vi rientrano i processi amministrativi preliminari, come le eventuali procedure di registrazione di aventi diritto di voto per l'ottenimento del materiale di voto al fine di partecipare al voto elettronico.

Il sistema comprende:

- La funzionalità di lettura dei dati del registro degli aventi diritto di voto necessari all'organizzazione degli scrutini elettronici.
- L'infrastruttura necessaria alla stampa del materiale di voto concepito appositamente per il voto elettronico.
- Le componenti con funzioni speciali importanti per la verificabilità del voto elettronico. Si tratta delle cosiddette componenti di controllo, delle componenti di setup, delle componenti di stampa e degli ausili tecnici dei verificatori.

Non fanno parte del sistema la tenuta del registro degli aventi diritto di voto, poiché non concerne specificamente il voto elettronico, e neppure il software di compilazione dei risultati parziali provenienti dai diversi canali di voto.

Lett. b: non appartengono al sistema online le componenti di sistema impiegate per la preparazione e lo spoglio (come la tipografia e la componente di setup).

Lett. c: un protocollo crittografico deve assicurare che in caso di disfunzioni o perfino di attacco le manipolazioni dei voti (modifica, aggiunta, eliminazione) possano essere rilevate anche se una sola componente di controllo per gruppo funziona correttamente. Inoltre, il segreto del voto deve essere preservato anche se una sola componente di controllo per gruppo funziona correttamente. Le modalità dettagliate figurano agli articoli 5–8, al numero 2 dell'allegato e nelle spiegazioni dettagliate. Il numero 3 dell'allegato contiene disposizioni concernenti l'attuazione tecnica e l'esercizio delle componenti di controllo volte a garantire che, per quanto possibile, tutte le componenti di controllo di un gruppo funzionino effettivamente in modo corretto. Quanto più componenti di controllo sono impiegate in un gruppo, quanto più esse si differenziano nell'attuazione tecnica, quanto più funzionano in modo indipendente le une dalle altre e quanto più sono protette dagli attacchi, tanto più alta è la probabilità che almeno una di esse funzioni correttamente.

Lett. d: i requisiti per la strutturazione e per l'esercizio indipendente sono riportati al numero 3 dell'allegato.

Lett. h: l'impiego di verificatori contribuisce alla trasparenza. Gli aventi diritto di voto devono poter partire dal presupposto che, caso di dubbio, possano rendere attenti i verificatori su irregolarità. L'impiego di verificatori in veste di rappresentanti degli aventi diritto di voto adempie l'articolo 27*m* capoverso 2 ODP (a tal proposito cfr. anche le relative spiegazioni). L'organizzazione concreta e le modalità di impiego dei verificatori sono rette dal diritto cantonale.

Lett. i: la piattaforma utente non fa parte dell'infrastruttura.

Lett. j: concerne in particolare l'implementazione dei seguenti processi:

- generare gli elementi segreti crittografici;
- verificare il diritto di voto (mediante i dati di autenticazione server si verifica se chi ha emesso il voto è una persona con diritto di voto; questa verifica può essere effettuata in modo anonimo);
- verificare la validità;
- registrare i voti in entrata;
- mischiare in modo crittografico i voti registrati;
- decrittare i voti;
- produrre le note di conferma che, mediante l'impiego delle componenti di controllo, risultano dalla garanzia della verificabilità individuale e dalla verificabilità universale.

Lett. m: in questo contesto la parte affidabile del sistema fa riferimento a un gruppo di componenti di controllo che fa parte del sistema online.

Lett. o n. 1: in un'elezione secondo il sistema maggioritario, i campi di testo libero sono sempre considerati come compilati conformemente al sistema.

Lett. p: sulla base dei dati di autenticazione client, l'ausilio tecnico utilizzato genera un messaggio di autenticazione (p. es. la firma di un voto) che è trasmesso all'infrastruttura; mediante il messaggio di autenticazione e i dati di autentificazione server (p. es. una chiave pubblica per verificare la firma), l'infrastruttura autentica il mittente di un voto come avente diritto di voto. I dai di autenticazione client devono essere difficili da indovinare.

Lett. r: nella prassi deve essere possibile generare un messaggio di autenticazione valido senza conoscere un dato di autenticazione client.

Lett. s: comprende ad esempio il certificato ISO 27001.

Art. 3 Condizioni di base per la concessione del nulla osta per il voto elettronico per ogni singolo scrutinio

Frase introduttiva, lett. a e c: le disposizioni sono rimaneggiate sotto il profilo redazionale. Inoltre, nella lettera a è stata integrata la verificabilità che secondo l'articolo 27*i* capoverso 1 ODP è ora richiesta per l'impiego di tutti i sistemi di voto elettronico.

Lett. a: concerne in particolare l'adempimento dei requisiti di cui agli articoli 4–9 OVE.

Lett. b: nell'attuazione di questa disposizione occorre in particolare prestare attenzione affinché il sistema sia concepito in modo tale da tenere conto delle esigenze specifiche degli aventi diritto di voto con disabilità (art. 27*g* cpv. 1 ODP). Il portale di voto elettronico deve pertanto essere privo di barriere e conforme alla norma di accessibilità eCH-0059 – ad eccezione del cap. 2.4 – e verificato da un servizio specializzato (cfr. n. 25.7.3 dell'allegato; controllo della conformità secondo n. 26.2.1 dell'allegato). Indicazioni per migliorare l'accessibilità del sistema possono essere presentate secondo l'articolo 13 capoverso 1 OVE. Inoltre, l'ODP prevede che nell'attuazione dei requisiti possano essere autorizzate agevolazioni per gli aventi diritto di voto con disabilità, sempre che la sicurezza non ne risulti sostanzialmente penalizzata (art. 27*g* cpv. 2 ODP).

Lett. c: concerne in particolare l'adempimento dei requisiti di cui agli articoli 10–12 OVE.

Lett. d: integrazione della disposizione vigente con una nuova condizione per l'accesso pubblico alle informazioni e per il coinvolgimento del pubblico (in particolare secondo gli art. 27*l*^{bis} e 27*l*^{ter} ODP e l'art. 13 OVE). Questa integrazione sottolinea l'importanza della trasparenza e del coinvolgimento del pubblico nel voto elettronico. Le informazioni da fornire dipendono dai gruppi di destinatari, in particolare il grande pubblico o le cerchie specialistiche.

Art. 4 Analisi dei rischi

Cpv. 1: per ottenere un'autorizzazione i Cantoni devono come finora effettuare un'analisi dei rischi nel loro ambito di responsabilità. Tutti i rischi connessi all'adempimento degli obiettivi di sicurezza devono essere determinati attraverso un'analisi dei rischi. Devono poi essere valutati anche rischi riguardanti il contesto del voto elettronico in seno all'amministrazione e al pubblico.

Le analisi dei rischi devono anche tenere conto del grado di fiducia nel voto elettronico e della sua accettazione da parte del pubblico. Si tratta di obiettivi sovraordinati che devono essere integrati in modo trasversale in tutti gli obiettivi e rischi di sicurezza. Qui di seguito sono riportati esempi di applicazione:

- esempio 1: si spiega come procedere nel caso in cui la verifica del risultato della votazione o dell'elezione sia negativa (p. es. mediante l'ausilio tecnico dei verificatori; cfr. art. 5 cpv. 3 lett. b OVE). Si tratta in tal modo di fugare eventuali dubbi sulla correttezza dei risultati;
- esempio 2: anche se sono scoperte soltanto lacune insignificanti, vi è il rischio che ne risulti incrinata la fiducia della popolazione. Per rimediarvi è possibile affidarsi a esperti indipendenti per classificare le lacune riscontrate (valutazione delle lacune, comunicazione).

Le analisi dei rischi devono avvenire conformemente a una metodologia che prevede le seguenti attività: identificare i rischi; analizzare i rischi; valutare i rischi. I dettagli della metodologia impiegata e i criteri di accettazione dei rischi predefiniti dal Cantone devono essere documentati. Le analisi dei rischi devono essere effettuate almeno una volta all'anno e in caso di modifiche sostanziali del sistema. Inoltre, prima di ogni scrutinio si deve verificare se vi sono nuovi rischi o se il livello dei rischi già noti si è innalzato.

Nell'ambito della sua valutazione della situazione la CaF può effettuare una propria analisi dei rischi presenti nel suo ambito di responsabilità. L'analisi dei rischi da parte della CaF non costituisce una condizione posta ai Cantoni per la concessione del nulla osta; una tale analisi può tuttavia essere considerata nella decisione sulla concessione del nulla osta. Essa è trasmessa ai Cantoni per conoscenza, in modo tale che questi possano considerare le valutazioni della CaF. Quest'ultima consulta le analisi dei Cantoni per stilare la propria analisi dei rischi.

La CaF mette a disposizione dei Cantoni una guida che illustra come effettuare le analisi dei rischi. Tutte le analisi dei rischi devono riflettere la situazione del momento e gli ultimi sviluppi e conoscenze devono costantemente esservi integrate.

Cpv. 2: il gestore o il fabbricante del sistema deve ora stilare una propria analisi dei rischi, in particolare se fa capo a un sistema esterno. Per altri fornitori di servizi rilevanti per la sicurezza, come ad esempio le tipografie o i fornitori di ausili tecnici per i verificatori o di componenti di controllo, il Cantone deve verificare se è sufficiente che effettui da sé un'analisi dei rischi o se è necessaria un'analisi supplementare da parte del fornitore del servizio. I fornitori di servizi stilano le analisi dei rischi destinate al Cantone. Quest'ultimo ne tiene conto per effettuare la propria analisi dei rischi, che sottopone alla Confederazione nell'ambito della procedura di autorizzazione.

Cpv. 3: rimaneggiamenti sotto il profilo linguistico della frase introduttiva e degli obiettivi di sicurezza nelle lettere a–e. L'attuale obiettivo di sicurezza della lettera f è precisato per chiarirne lo scopo. Rientra ad esempio in questo obiettivo di sicurezza il tema della compravendita di voti.

Cpv. 4: corrisponde essenzialmente al vigente capoverso 2. L'obbligo di specificare le ragioni per le quali i rischi sono ritenuti sufficientemente bassi è stato ripreso al capoverso 1.

Il vigente capoverso 3 può essere stralciato perché secondo l'articolo 11 OVE i documenti devono essere pubblicati integralmente; la disposizione diviene pertanto priva di significato.

Art. 5 Requisiti posti alla verificabilità completa

La verificabilità completa garantisce che, nel rispetto del segreto del voto, siano riconosciute disfunzioni sistematiche nello svolgimento delle elezioni e votazioni a seguito di errori di software, operazioni umane errate o tentativi intenzionali di manipolazione. In questo contesto rientra pure necessariamente la nota di conferma che l'elettore riceve secondo la quale il suo voto ha raggiunto la parte affidabile del sistema senza alterazioni e non è stato manipolato, ad esempio mediante un programma nocivo presente sul computer impiegato. I verificatori possono assicurarsi, indipendentemente dal sistema impiegato, che tutti i voti di cui è stato possibile accertare che sono stati emessi correttamente dagli aventi diritto di voto siano stati anche conteggiati correttamente, ovvero conformemente alla nota di conferma che i votanti hanno ricevuto. L'attuazione della verificabilità completa deve fondarsi su metodi crittografici riconosciuti.

In futuro saranno autorizzati soltanto sistemi con verificabilità completa. Le condizioni di cui ai vigenti articoli 4 e 5 sono recepite con alcuni rimaneggiamenti negli articoli 5–8 OVE.

Cpv. 2: la verificabilità individuale consente agli aventi diritto di voto di constatare qualsiasi utilizzazione abusiva, intenzionale o involontaria, del loro diritto di voto. Ciò dev'essere possibile anche quando la piattaforma utente e la via di trasmissione non siano affidabili. Concretamente, si deve presumere a priori l'esistenza di virus non individuabili o di altri interventi sulla piattaforma utente o sulla via di trasmissione. Il voto quale è stato immesso dal votante nella piattaforma utente corrisponde sempre alla volontà del votante, salvo che questi abbia commesso un errore al momento dell'immissione.

Cpv. 3: la verificabilità universale consente di individuare ogni manipolazione, intenzionale o involontaria, nell'infrastruttura (modifica, aggiunta, eliminazione). Contrariamente alla verificabilità individuale, la possibilità di una verifica universale non deve necessariamente essere offerta agli aventi diritto di voto. Possono invece essere impiegati verificatori che mettono in atto la verificabilità universale. Il processo di verifica deve essere osservabile, ovvero i verificatori devono essere in grado di comprendere per quanto possibile il significato e i risultati delle differenti tappe. A tal fine, devono poter attestare l'esecuzione corretta delle tappe e dei risultati dei test, ad esempio recandosi sul luogo dell'esecuzione.

Art. 6 Validità delle note di conferma

Nessuna nota può confermare con assoluta certezza che i voti siano stati trattati in modo corretto conformemente ai requisiti di cui all'articolo 5 capoversi 2 e 3 OVE. Le note di conferma devono dunque essere intese nell'ottica della loro validità. L'articolo 6 OVE menziona a tal proposito requisiti minimi di cui fidarsi nell'interpretare una nota di conferma. Più la validità è elevata, più la falsificabilità è improbabile. Nell'allegato dell'OVE figurano precisazioni e ulteriori requisiti posti alla validità (n. 2.9.1, 2.9.2 e 2.11). L'elenco di cui alle lettere a–c dell'articolo 6 è esaustivo. In tal modo per la validità delle note di conferma secondo l'articolo 5 è determinante esclusivamente l'affidabilità secondo le lettere a–c.

Un avente diritto di voto che si avvale della verificabilità individuale dovrebbe poter essere certo, sulla base del riferimento di verificabilità recapitato per posta, che il suo voto è in tutta probabilità giunto a destinazione, sempre che la produzione e la stampa dei dati per il riferimento della verifica siano avvenuti in modo regolare e che una delle quattro componenti di controllo funzioni correttamente (cfr. le spiegazioni concernenti il n. 2 dell'allegato). Per l'avente diritto di voto che non credesse che queste condizioni siano soddisfatte, il risultato dell'esame della conferma rivestirebbe dunque scarso significato o sarebbe del tutto insignificante. Questo significa che per questa persona la nota di conferma non è sufficientemente valida.

Il corretto funzionamento della piattaforma utente degli aventi diritto di voto e la via di trasmissione non devono costituire presupposti per la validità della nota di conferma secondo l'articolo 5 capoverso 2 lettera a OVE. Questo significa che la nota di conferma deve essere valida anche se una piattaforma utente è stata manipolata o un *man-in-the-middle*[9] ha manipolato di nascosto il voto: grazie alla nota di conferma secondo l'articolo 5 capoverso 2 OVE l'avente diritto di voto può comunque constatare la manipolazione.

Analogamente alla validità della nota di conferma secondo il capoverso 3: la nota di conferma è valida se consente ai verificatori di constatare manipolazioni tenuto conto delle ipotesi di fiducia formulate. Questo impedisce all'aggressore di ingannare i verificatori utilizzando componenti non affidabili del sistema per fabbricare una nota di conferma che legittimi un risultato manipolato. Fintanto che i verificatori hanno la certezza che una delle quattro componenti di controllo e l'ausilio tecnico da essi utilizzato per verificare le prove funzionano correttamente (in genere un computer portatile), le note di conferma sono valide.

Art. 7 Tutela del segreto del voto ed esclusione di risultati parziali anticipati

Per tutelare il segreto del voto ed escludere risultati parziali anticipati il sistema deve essere configurato in modo tale che sia necessario prendere il controllo di tutte le componenti di controllo affinché dopo l'espressione del voto un'aggressione vada a buon fine. Se un sistema online è gestito da un gestore privato, si applicano requisiti più stringenti. Precisazioni a tal proposito sono riportate nell'allegato dell'OVE (n. 2.9.3).

Art. 8 Requisiti posti alla parte affidabile del sistema

Questi requisiti servono affinché un accesso non autorizzato riuscito non agevoli per quanto possibile il tentativo di accedere di nascosto a un'altra componente di controllo.

Art. 9 Misure supplementari per ridurre i rischi

Questo articolo corrisponde, con alcune modifiche redazionali, al vigente articolo 6 OVE. Esso stabilisce che se, nonostante le misure prese per adempiere le condizioni dell'OVE (soprattutto secondo gli art. 3 e 5–8 OVE), i rischi non risultano sufficientemente bassi, occorre adottare misure supplementari. La nozione di «sufficientemente bassi» si riferisce ai criteri di valutazione e di accettazione dei rischi definiti dai Cantoni e dalla CaF.

Art. 10 Requisiti posti alla verifica

Per aumentare l'efficacia delle verifiche e l'indipendenza fra l'organo incaricato della verifica e quello sottoposto a verifica, la suddivisione dei compiti fra la Confederazione e i Cantoni è modificata in modo tale che la Confederazione assuma maggiori responsabilità e un ruolo più diretto nella verifica dei sistemi. Le verifiche saranno in futuro commissionate in gran parte dalla CaF (cpv. 1; cfr. anche il commento all'art. 27*l* cpv. 3 e 4 ODP). In questi settori si rinuncia a una certificazione da parte di organi accreditati dal Servizio di accreditamento svizzero (SAS). Il Cantone continua a provvedere affinché una verifica in relazione con l'esercizio del sistema sia condotta nel centro di calcolo del gestore del sistema (cpv. 2). Gli ulteriori requisiti, come l'oggetto, i criteri d'esame, le competenze e i termini per le verifiche, continuano ad essere disciplinati nell'allegato all'OVE (n. 26).

Cpv. 1 lett. b: adeguamento della designazione; la nuova designazione è «software del sistema». Questa verifica comprende la precedente verifica secondo i numeri 5.2 (funzionalità) e 5.4 (componenti di controllo) dell'allegato. Con la nuova formulazione sono verificati assieme il software dell'intero sistema e delle componenti di controllo.

[9] Designa l'aggressore che conduce un *attacco man in the middle* (MITM). Si tratta di una forma di attacco utilizzata nelle reti di computer. L'aggressore si intromette fisicamente o, come succede più spesso attualmente, per via informatica fra due parti in comunicazione fra loro e con il suo sistema esercita un controllo totale sui dati scambiati fra due o più partecipanti della rete. L'aggressore può in tal modo leggere le informazioni e addirittura manipolarle a suo piacimento.

Cpv. 1 lett. c: i requisiti applicabili alle tipografie rientrano ora nella disposizione «sicurezza dell'infrastruttura e dell'esercizio». L'infrastruttura e l'esercizio possono essere suddivisi tra il gestore del sistema e i Cantoni. Questa ripartizione dipende dal sistema scelto e dal modello di collaborazione. Tutti gli elementi dell'infrastruttura e tutti gli aspetti dell'esercizio sono esaminati. L'esame è effettuato presso l'organo responsabile dell'elemento in questione.

Cpv. 2: la gestione del sistema nel centro di calcolo del gestore del sistema deve essere certificata conformemente alla norma ISO 27001. Questa verifica è lasciata ai Cantoni perché si basa su uno standard riconosciuto e vi è un metodo definito per la sua esecuzione. Un Cantone che non gestisce da sé un sistema può farsi certificare per i processi cantonali conformemente alla norma ISO 27001, ma non è obbligato a farlo.

Cpv. 3: la CaF e gli enti incaricati dello svolgimento della verifica secondo il capoverso 1 devono avere accesso ai necessari documenti presso i Cantoni e i suoi fornitori di servizi. Tra questi figurano tutti i documenti necessari per la verifica secondo il capoverso 1 e tutti i rapporti disponibili (inclusi i rapporti di certificazione), gli attestati e i certificati (certificato ISO 27001 secondo il capoverso 2 ed eventuali certificati cantonali).

Cpv. 4:

- I risultati delle verifiche che sono rilevanti per l'autorizzazione sono pubblicati. L'ente competente pubblica gli attestati e i certificati che sono stati allestiti nell'ambito delle verifiche secondo i capoversi 1 e 2. Tra gli attestati rientrano anche i rapporti di verifica. Per quanto riguarda le verifiche secondo il capoverso 2 occorre almeno pubblicare la Dichiarazione di applicabilità (Statement of Applicability, SoA); altrimenti vanno pubblicati i risultati completi.
- I rapporti di verifica pubblicati devono essere comprensibili. Se fanno riferimento ad altri documenti, questi ultimi devono di norma essere pubblicati. Se non è possibile pubblicare documenti supplementari, i risultati delle verifiche devono essere resi comprensibili mediante una descrizione sommaria degli aspetti rilevanti della documentazione non pubblicata.
- Se l'ente sottoposto a verifica formula una replica a un rapporto di verifica e auspica che sia pubblicata, la replica è pubblicata dall'ente competente secondo i capoversi 1 e 2.
- Per la pubblicazione è responsabile l'ente che ha commissionato la verifica. Per le verifiche secondo il capoverso 1 è competente la CaF, per le verifiche secondo il capoverso 2 il Cantone o il gestore del sistema.
- Per quanto riguarda la deroga al principio della pubblicazione si veda il commento all'articolo 27*l*^{bis} capoverso 3 ODP.

Art. 11 Pubblicazione del codice sorgente e della documentazione relativa al sistema e al suo esercizio

Le condizioni vigenti per la pubblicazione del codice sorgente e dei documenti concernenti il sistema e il suo esercizio sono precisate. Il capoverso 1 contiene un nuovo elenco di documenti che devono essere pubblicati. Qui di seguito alcune spiegazioni di termini utilizzati:

Cpv. 1 lett. a: i «parametri rilevanti» comprendono tutte le informazioni e i dati che sono necessari affinché le persone interessate possano mettere il sistema in servizio presso di sé.

Cpv. 1 lett. c: la documentazione del software comprende in particolare il protocollo crittografico, la specificazione e la concezione, le istruzioni, i concetti del test, i rapporti concernenti lacune e correttivi, nonché i risultati di esami svolti nell'ambito dello sviluppo del sistema (p. es. *code review*, rapporti di test).

Cpv. 1 lett. d: comprende i documenti che illustrano il processo di sviluppo (cfr. il commento all'art. 27*l*^{bis} cpv. 2 lett. c ODP).

Cpv. 1 lett. e: comprende documenti che agevolano la messa in servizio del sistema per testarlo (p. es. istruzioni, FAQ, ecc.).

Cpv. 1 lett. f: per «principali componenti» s'intendono le componenti il cui corretto funzionamento è importante per la riduzione dei rischi, in particolare le componenti affidabili secondo il numero 2 dell'allegato. Le specifiche tecniche comprendono il nome del fabbricante e la designazione del prodotto, nonché le

informazioni pertinenti per l'identificazione delle lacune di sicurezza (p. es. versione del sistema d'esercizio o del firmware, versione dell'ambiente Java-Runtime).

Cpv. 1 lett. g: comprende documenti che attestano la conformità ai requisiti dell'OVE. Vi figurano documenti che illustrano le misure essenziali di riduzione dei rischi menzionate nell'analisi dei rischi. Vale il principio che più la documentazione concerne l'esercizio, la manutenzione o la sicurezza di una parte affidabile del sistema secondo il numero 2 dell'allegato o la manipolazione di un supporto con dati critici, più è importante procedere alla pubblicazione. Inoltre, valgono le deroghe previste dalle disposizioni della legislazione in materia di trasparenza.

Cpv. 1 lett. h: se il gestore del sistema viene a conoscenza di una lacuna nel codice sorgente pubblicato o nella documentazione, deve darne notizia descrivendo la lacuna e le eventuali misure adottate per porvi rimedio. Questo contribuisce alla comprensibilità, alla trasparenza e alla cooperazione con il pubblico.

Cpv. 2 lett. c: come indicato nel commento all'articolo 27*l*bis capoverso 3 ODP, le deroghe motivate si fondano in particolare sul diritto in materia di trasparenza o di protezione dei dati. Inoltre, per quanto riguarda la pubblicazione secondo l'articolo 11, in casi motivati è possibile prescindere dalla pubblicazione di documenti non rilevanti o scarsamente rilevanti per la sicurezza del sistema e dell'esercizio, come descrizioni di processi operativi senza un legame diretto con il sistema oppure semplici precisazioni irrilevanti o di scarso rilievo per la sicurezza o che si deve ritenere siano state attuate correttamente. Se sono richieste deroghe, occorre procedere a una ponderazione degli interessi (cfr. commento all'art. 27*l*bis cpv. 3 ODP).

Art. 12 Modalità di pubblicazione

Le esigenze in materia di trasparenza e accessibilità relative alle informazioni concernenti il sistema e il suo funzionamento devono di principio essere elevate. L'OVE non impone che i documenti siano pubblicati con una licenza *open source*. Tuttavia, nel 2020, Confederazione e Cantoni si sono pronunciati a favore di una pubblicazione con licenza *open source* dei futuri sistemi e componenti del sistema[10]. Il presente disciplinamento nell'OVE per la pubblicazione dei documenti ha lo scopo di indurre il più gran numero possibile di esperti indipendenti a occuparsi dei documenti pubblicati.

Cpv. 1: i documenti devono essere pubblicati su piattaforme correnti. I file devono essere organizzati tenendo conto dell'ampiezza e della complessità della prassi corrente.

Cpv. 2: i documenti pubblicati devono poter essere ottenuti in modo anonimo e il proprietario del codice sorgente non deve invitare le persone interessate a registrarsi per ricevere i documenti. Se una persona ha diritto a una remunerazione conformemente all'articolo 13 OVE, il proprietario può richiedere le informazioni necessarie per il versamento. Si ritiene opportuno provvedere alla pubblicazione circa sei mesi prima dell'impiego del sistema, in modo da consentire una verifica efficace da parte del pubblico.

Cpv. 3: lo scambio con altre persone e la citazione di informazioni pubblicate devono essere possibili, in particolare per facilitare la ricerca di lacune da parte degli specialisti.

Cpv. 4 lett. b: al fine di garantire una divulgazione responsabile (*responsible disclosure*) il proprietario può esigere che vengano rispettate le regole seguenti:

- segnalare immediatamente lacune al proprietario del codice sorgente;
- rispettare un dato termine prima di segnalare pubblicamente una lacuna;
- adottare un approccio responsabile riguardo alle informazioni concernenti lacune presunte. Non si diffondono inutilmente informazioni su potenziali falle nella sicurezza. Le informazioni sono condivise e discusse soltanto con persone che si suppone siano in grado e disposte a trattare la questione e adottino anch'esse un approccio responsabile.

Cpv. 5: se il proprietario del codice sorgente stabilisce condizioni di utilizzo per il codice sorgente e la documentazione (p. es. esclusione di un utilizzo commerciale da parte di terzi) oppure condizioni secondo il capoverso 4 lettera b (condizioni per la trasmissione di segnalazioni secondo l'art. 13 cpv. 1 OVE), le

[10] Cfr. la misura C.2 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

violazioni di tali condizioni possono essere sanzionate soltanto nei casi eccezionali menzionati nel capoverso 5 (se qualcuno utilizza il codice sorgente o parti di esso per scopi commerciali o di produzione). Nelle condizioni di utilizzo il proprietario del codice sorgente deve attirare l'attenzione sulle limitazioni per quanto riguarda le possibilità di sanzionare. Si rinuncia a richiedere una dichiarazione d'intenti ai partecipanti.

Art. 13 Coinvolgimento del pubblico

Il presente articolo disciplina i principi di un programma *bug bounty*, una misura introdotta per attuare l'articolo 27*l*ter ODP. Per quanto possibile i Cantoni devono adottare ulteriori misure per definire incentivi sia finanziari che di altro genere.

Cpv. 1: in linea di principio i Cantoni provvedono affinché le persone interessate del pubblico possano trasmettere segnalazioni volte a migliorare il sistema (programma *bug bounty*). Il programma *bug bounty* dovrà essere avviato per tempo prima che sia presentata al Consiglio federale una domanda definitiva per l'autorizzazione di principio. È ritenuto ragionevole un termine di circa sei mesi prima dell'impiego previsto. Il programma *bug bounty* prevede un programma permanente per la ricerca di errori (lett. a) e un test Internet ricorrente (lett. b).

Cpv. 1 lett. a: ricerca di errori nella documentazione o nel codice sorgente pubblicati e ricerca di errori mediante l'analisi del sistema operativo nella propria infrastruttura. Questo programma per la ricerca di errori funziona ininterrottamente.

Cpv. 1 lett. b: lo scopo di questo cosiddetto test Internet è esclusivamente quello di penetrare nell'infrastruttura. Gli attacchi di negazione del servizio (*denial of service*) e gli attacchi di ingegneria sociale (*social engineering*) possono essere esclusi dal programma *bug bounty*. Il test Internet può essere attuato come programma permanente o come test ricorrente di durata limitata.

La partecipazione al programma *bug bounty* è disciplinata dall'articolo 12 OVE.

L'organo designato per gestire il programma *bug bounty* può essere un organo interno del Cantone stesso, il gestore del sistema o un'impresa esterna.

Cpv. 2: l'organo competente permette l'attuazione del programma, riceve le segnalazioni e assicura la comunicazione con la persona che ha effettuato la segnalazione. Esso deve essere informato sulle decisioni in merito alla segnalazione e sulle eventuali misure.

Inoltre, dovranno essere pubblicate le informazioni sulle segnalazioni ricevute. Le informazioni da pubblicare sono le seguenti: informazioni sul contenuto della segnalazione, fonte della segnalazione (sempre che la persona o l'istituzione che l'ha fatta acconsenta), valutazione da parte dell'organo responsabile del programma *bug bounty* e informazioni su misure eventualmente adottate sulla base della segnalazione.

Cpv. 3: oltre alle segnalazioni che riguardano direttamente la sicurezza, devono essere remunerate anche quelle con una relazione indiretta, purché contribuiscano a migliorare il sistema. Le segnalazioni con una relazione indiretta sono per esempio quelle che consentono di migliorare la qualità del codice sorgente. In effetti, la qualità del codice sorgente è tra l'altro determinante per la leggibilità e dunque anche per la probabilità di scovare errori. L'ammontare della remunerazione finanziaria deve essere fissato secondo l'importanza della lacuna e dovrà essere sufficientemente elevato per incitare effettivamente le persone del pubblico con le necessarie conoscenze specialistiche a partecipare.

Le basi legali della CaF definiscono soltanto le condizioni quadro del programma *bug bounty*. Le modalità in dettaglio del programma, ad esempio la definizione di categorie che consentano di valutare la gravità delle lacune o stabilire la remunerazione finanziaria, rientrano nella sfera di competenza dei Cantoni o del gestore del sistema. La Confederazione verifica nell'ambito della procedura di autorizzazione in che misura la procedura scelta dai Cantoni e dall'organo competente secondo il capoverso 1 abbia permesso di raggiungere gli obiettivi del programma *bug bounty*.

Art. 14 Responsabilità e competenze per il corretto svolgimento degli scrutini per via elettronica

I compiti e le responsabilità sono stati finora disciplinati nell'allegato. La loro ripartizione è ora disciplinata nella parte principale dell'OVE.

Cpv. 2: questa disposizione si applica in particolare ai compiti seguenti:

- Compiti dell'organo competente a livello cantonale secondo il capoverso 3.
- Concezione del materiale di voto e definizione delle informazioni che deve contenere.
- Esercizio della componente di setup e di almeno una componente di controllo del gruppo che comprende una parte della chiave di decrittazione dei voti (cfr. n. 3.1 dell'allegato).
- Decrittazione e spoglio dei voti (n. 11.2 dell'allegato).
- Comunicazione con gli aventi diritto di voto su questioni concrete relative al voto.

Fatti salvi i compiti importanti, il Cantone può delegare i compiti menzionati a organizzazioni esterne, anche se continua a mantenere la responsabilità generale secondo il capoverso 1. Esso assume dunque ad esempio integralmente i rischi connessi all'esecuzione di un compito anche se lo ha delegato. In deroga ai compiti importanti, che il Cantone deve eseguire da sé, la comunicazione su questioni concernenti il funzionamento del sistema può essere delegata quando si tratta di aspetti molto tecnici che necessitano di conoscenze specialistiche.

Cpv. 3: i compiti dell'organo responsabile a livello cantonale sono al momento disciplinati nell'allegato. In futuro saranno disciplinati nella parte principale dell'OVE.

Cpv. 3 lett. a: la direttiva sovraordinata in materia di sicurezza dell'informazione può essere una direttiva generale di un Cantone o una direttiva applicabile specificamente al voto elettronico. Essa definisce gli obiettivi, il quadro e le responsabilità per quanto riguarda la sicurezza dell'informazione. Comprende anche un catalogo di direttive per la sicurezza dell'informazione a livello inferiore e precisa le modalità della sua gestione. È comunicata a tutti collaboratori e deve essere verificata e adeguata a scadenze regolari.

Cpv. 3 lett. b: la direttiva in materia di classificazione ed elaborazione delle informazioni definisce un quadro di sicurezza vincolante per l'esercizio generale del sistema. È comunicata ai collaboratori interessati e deve essere verificata e adeguata a scadenze regolari.

Cpv. 3 lett. c: la direttiva in materia di gestione dei rischi definisce in particolare il campo d'applicazione e i limiti della gestione dei rischi relativi alla sicurezza dell'informazione, l'organizzazione della gestione dei rischi, i criteri sulla sostenibilità dei rischi e il metodo per effettuare un'analisi dei rischi. Deve essere verificata e adeguata a scadenze regolari.

Cpv. 3 lett. d: esempi di misure: effettuare un'analisi dei rischi, verificare la conformità con le direttive in materia di sicurezza dell'informazione, rielaborare direttive in materia di sicurezza dell'informazione, mettere a disposizione strumenti adeguati.

Cpv. 3 lett. f: per «atti e operazioni critici» s'intendono in particolare la preparazione dello scrutinio (n. 5 dell'allegato), l'apertura e la chiusura del canale di voto elettronico (n. 9 dell'allegato), lo spoglio dei voti depositati nell'urna elettronica (n. 11 dell'allegato) e la distruzione dei dati dopo l'omologazione dei risultati delle votazioni e delle elezioni (n. 12.8 dell'allegato).

Cpv. 3 lett. h: la determinazione dei verificatori e l'organizzazione e le modalità concrete del loro impiego sono rette dal diritto cantonale. L'organo responsabile a livello cantonale accompagna i verificatori nel loro impiego e li istruisce. Oltre a una formazione, l'istruzione dei verificatori comprende lo svolgimento di esercizi.

Cpv. 3 lett. i: oltre ad altri indicatori, secondo il numero 11.10 dell'allegato devono essere comunicati ai verificatori il numero e il tipo di anomalie che gli aventi diritto di voto hanno segnalato al Cantone.

Cpv. 4: gli organi preposti all'esercizio operano su istruzione del Cantone e si assumono nei suoi confronti la responsabilità del loro operato.

Cpv. 5: l'organizzazione e le modalità concrete dell'impiego dei verificatori sono rette dal diritto cantonale.

Art. 15 Documenti relativi alle domande

Cpv. 1: a seguito della modifica dell'articolo 27*b* lettera b ODP sono qui disciplinati unicamente i documenti da allegare alla domanda per ottenere il nulla osta. Le ulteriori informazioni da fornire nella domanda per di rilascio di un'autorizzazione di principio sono menzionate nell'articolo 27*c* ODP.

Il Cantone può far valere la validità di risultati di verifiche o di attestati per diversi scrutini (sul termine «valido» cfr. anche il commento al cpv. 2). In questo caso il Cantone giustifica per quale motivo, riguardo allo scrutinio interessato, non è necessario ripetere la verifica. Indica tutte le modifiche apportate o previste al sistema o ai processi di esercizio e di manutenzione fino al momento dello scrutinio, mostrando così che si tratta di adeguamenti di minore importanza che non hanno alcun influsso negativo sull'analisi dei rischi.

Tra le attuali informazioni sul pianificato impiego del voto elettronico che devono essere presentate nell'ambito della procedura di autorizzazione figurano ad esempio le versioni del sistema e le componenti del sistema da impiegare, la descrizione e le spiegazioni su eventuali divergenze rispetto alle versioni esaminate, lo scadenzario degli scrutini pianificati e le indicazioni attuali sull'organizzazione concreta della cellula di crisi.

Per quanto riguarda gli attestati per l'adempimento dei requisiti legali, nell'ambito della procedura di autorizzazione devono in particolare essere presentati gli attestati che non rientrano nella verifica su mandato della CaF. Si tratta, ad esempio, di informazioni sulla comunicazione prevista con gli aventi diritto di voto secondo l'articolo 27*m* capoverso 1 ODP, il controllo della plausibilità dei risultati secondo l'articolo 27*i* capoverso 2 ODP previsto o già effettuato, la pubblicazione dei risultati espressi per via elettronica secondo l'articolo 27*m* capoverso 3 ODP prevista o già effettuata, nonché i documenti di cui alle lettere a–e. Questo elenco degli attestati comprende – con adeguamenti alle nuove disposizioni dell'OVE – il precedente articolo 8 capoverso 1 OVE e l'elenco figurante al numero 6 della precedente versione dell'allegato dell'OVE affinché ci sia un elenco unico degli attestati. I termini precisi e ulteriori dettagli saranno definiti dalla CaF in un documento separato.

Cpv. 1 lett. a: il Cantone presenta analisi dei rischi attuali del Cantone e se del caso dei suoi fornitori di servizi secondo l'articolo 4 OVE. Il Cantone si impegna a segnalare immediatamente qualsiasi cambiamento nell'analisi dei rischi.

Cpv. 1 lett. b: secondo le competenze in materia di verifica dei sistemi e del loro esercizio, i Cantoni presentano i certificati e i relativi allegati che hanno allestito nell'ambito delle loro verifiche secondo l'articolo 10 capoverso 2 OVE, nonché gli attestati per l'adempimento dell'obbligo di pubblicazione secondo l'articolo 10 capoverso 4 OVE.

Cpv. 1 lett. c: il Cantone presenta attestati per confermare che i documenti di cui all'articolo 11 OVE siano stati pubblicati. Informa pure la CaF sulle date in cui i documenti sono stati pubblicati. Inoltre, comunica informazioni sulle segnalazioni ricevute dal pubblico: un elenco delle segnalazioni ricevute, la loro valutazione da parte del Cantone o dell'organo competente, l'ammontare della remunerazione finanziaria corrisposta e una descrizione delle misure adottate sulla base di tali segnalazioni.

Cpv. 1 lett. d: si riprende il precedente numero 6.3 dell'allegato dell'OVE. Se un test è effettuato soltanto nell'imminenza dello scrutinio, il Cantone sottopone altri verbali relativi al test. Se il sistema presenta lacune di cui il Cantone o il gestore del sistema hanno conoscenza, la CaF deve essere informata di tali lacune, dei loro effetti e delle misure previste.

Cpv. 2: il termine «valido» va inteso nel suo significato stretto (come ad esempio per la validità di un certificato) e nel suo significato largo (documenti che non sono stati adeguati e che non devono essere adeguati, per esempio perché la concezione del sistema, lo stato delle conoscenze tecniche o le basi legali non hanno subito modifiche). In caso di rimando si dovrà motivare e confermare che i documenti sono sempre validi.

Art. 16 Ulteriori disposizioni

Cpv. 2: in casi particolari un Cantone può essere dispensato dall'adempiere determinati requisiti purché ottemperi ai tre requisiti elencati alle lettere a–c. Deve in particolare illustrare in modo comprensibile per quale ragione non ha ottemperato a tali requisiti. Per esempio, in uno scrutinio con sistema maggioritario

non c'è l'obbligo di conformarsi ai requisiti relativi alla verificabilità individuale se, per emettere un voto, si deve inserire un nome in un campo libero.

4.2.2 Allegato con i requisiti tecnici e amministrativi posti al voto elettronico

Osservazione generale

Il rimando al profilo di sicurezza dell'Ufficio federale della Germania per la sicurezza informatica (*Bundesamt für Sicherheit in der Informationstechnik*, BSI precedente n. 3.15) è stato eliminato dato che tale profilo non è più gestito dal BSI ed è stato archiviato. I requisiti rilevanti del profilo di sicurezza sono stati inclusi puntualmente nei requisiti esistenti o in nuovi requisiti.

Spiegazioni concernenti parte delle disposizioni

N. 1 Definizioni

N. 1.3: Il votante confronta i codici visualizzati sullo schermo con quelli del riferimento di verifica.

N. 2 Requisiti posti al protocollo crittografico per la verificabilità completa (art. 5)

Tra il momento dell'operazione di voto e quello del conteggio, i voti elettronici si spostano dalle piattaforme utenti al Cantone attraverso Internet e i numerosi server del gestore del sistema. Gli elementi dell'infrastruttura utilizzata sono numerosi e difficilmente controllabili. I protocolli crittografici permettono di ridurre al minimo il numero di elementi che potrebbero agevolare un aggressore nel modificare voti senza essere notato o violare il segreto del voto. Le misure per evitare incursioni da parte di un aggressore possono quindi concentrarsi in modo mirato su questi elementi circoscritti. Si tratta di elementi particolarmente degni di protezione e, idealmente, che possono anche essere protetti in modo particolarmente efficace e dissuasivo. Vigono in tal senso i requisiti di cui al numero 3.

Questi elementi – che si trovano tra i partecipanti al sistema e i canali di comunicazione elencati nei numeri 2.1 e 2.2 – sono descritti come «affidabili». A prima vista questa associazione potrebbe risultare sorprendente: perché designare «affidabile» un elemento particolarmente degno di protezione? La spiegazione va ricercata nel fatto che lo scopo dei protocolli crittografici non è quello di proteggere tali elementi. La designazione «affidabile» segnala agli autori e ai lettori del documento contenente il protocollo crittografico che non devono preoccuparsi di possibili attacchi in cui un aggressore prende il controllo di questi elementi. Essendo affidabili, i partecipanti al sistema si rifiutano di cooperare con un aggressore. Il protocollo deve essere definito in modo tale che – finché i partecipanti affidabili al sistema si attengono al protocollo – l'aggressore non avrà successo, anche se porta gli altri partecipanti non affidabili al sistema sotto il suo controllo. L'uso del termine affidabile è basato sulla letteratura specifica in materia.

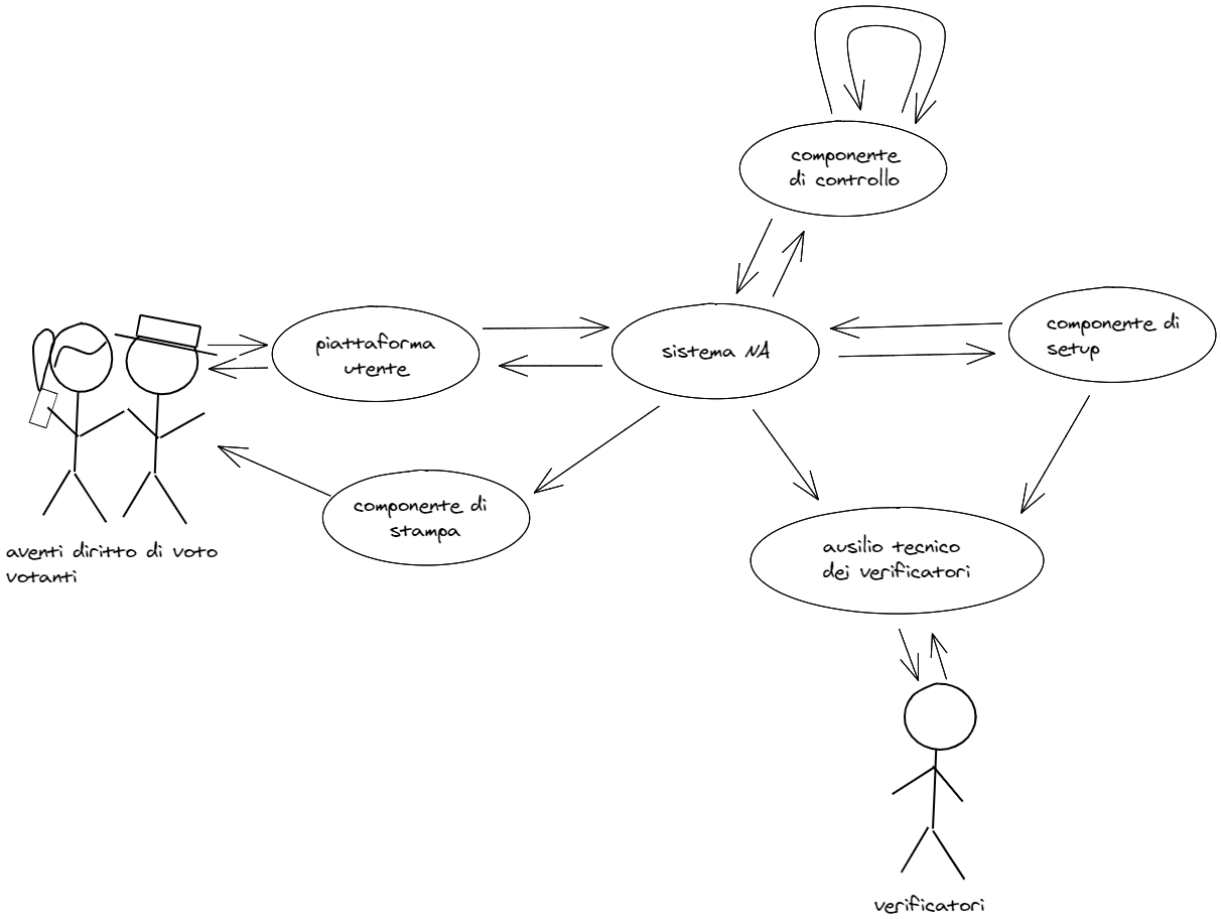
Il protocollo crittografico consiste in istruzioni astratte, scritte in linguaggio matematico, destinate a tutti i partecipanti al sistema e che indicano i calcoli che questi devono eseguire quando ricevono i vari messaggi, i dati che devono salvare e i messaggi che devono inviare attraverso quali canali. Il protocollo è conforme con l'OVE se l'aggressore secondo il numero 2.3 non può pregiudicare gli obiettivi di cui ai numeri 2.5–2.8 alle condizioni di cui ai numeri 2.11 e 2.12, nonostante il suo controllo sui partecipanti al sistema non affidabili e sui canali di comunicazione di cui ai numeri 2.1, 2.2, 2.9 e 2.10. Il numero 2.13 richiede da un lato l'uso di elementi crittografici sicuri (ad esempio algoritmi crittografici) e dall'altro che le istruzioni date ai partecipanti al sistema siano chiare e sufficientemente precise. Il numero 2.14 richiede note di conferma matematiche della conformità del protocollo (note di conformità), conformemente all'usuale prassi scientifica.

Il protocollo crittografico è la base per lo sviluppo del sistema. Può essere efficace solo se le istruzioni concernenti gli elementi affidabili sono correttamente implementate in forma di software e se le componenti alla base del software sono sufficientemente protette. L'OVE contiene requisiti a questo proposito. Cfr. in merito anche il commento concernente i numeri 2.3 e 2.4.

N. 2.1:

- Avente diritto di voto / votante: gli aventi diritto di voto ricevono per posta dal Cantone o dalla tipografia, prima dello scrutinio, le caratteristiche di autenticazione client e il riferimento di verifica, entrambi confidenziali. Per trasmettere un voto, inseriscono nella piattaforma utente le caratteristiche di autenticazione client e il loro voto. Per la verificabilità individuale secondo l'articolo 5 OVE in combinato disposto con il numero 2.5 dell'allegato OVE, verificano che le note di conferma indicate nella piattaforma utente corrispondano al riferimento di verifica ricevuto per posta.
- Piattaforma utente: la piattaforma utente crea i messaggi di autenticazione e li invia al sistema non affidabile (sistema NA) insieme al voto crittato e ad altri messaggi necessari per garantire la verificabilità. A tal fine utilizza il software aggiuntivamente ai parametri pubblici che ha ricevuto in precedenza dal sistema NA. Nella piattaforma utente il votante visualizza i messaggi trasmessi dal sistema NA (ad es. le note di conferma di cui al n. 2.5).
- Componente di setup: la componente di setup è gestita nell'infrastruttura del Cantone (cfr. n. 3.1). Con l'aiuto della componente di setup, il Cantone prepara i dati per lo svolgimento degli scrutini. Ciò include, in particolare, i dati la cui casualità e confidenzialità sono cruciali per raggiungere i requisiti posti al protocollo crittografico di cui ai numeri 2.5, 2.7 e 2.8, come ad esempio il riferimento di verifica degli aventi diritto di voto. Anche questo termine astratto può includere diversi ausili tecnici come computer portatili e supporti di dati.
- Sistema non affidabile (sistema NA): funge da nodo di comunicazione tra gli altri partecipanti al sistema. Deve essere considerato non affidabile in relazione a tutti i requisiti posti al protocollo crittografico (cfr. n. 2.9).
- Componente di stampa: stampa il riferimento di verifica che sarà trasmesso agli aventi diritto di voto. Questo termine astratto include l'imballaggio e la spedizione agli elettori. Inoltre, include tutti gli ausili tecnici utilizzati per la stampa. Oltre alla stampante stessa dunque anche un computer portatile per decrittare i dati di stampa e una chiavetta USB per memorizzare i dati crittati.
- Uno o più gruppi di componenti di controllo: le componenti di controllo interagiscono con le altre componenti di controllo del loro stesso gruppo in modo tale che i requisiti posti al protocollo crittografico secondo i numeri 2.5, 2.6 e 2.7 sono soddisfatti anche se solo una di loro è affidabile e quindi funziona correttamente.
- Verificatori: dopo il conteggio, i verificatori ricevono da parte del sistema NA una nota di conferma secondo il numero 2.6 a conferma del corretto accertamento del risultato. Eseguono la verifica dopo l'accertamento del risultato con un ausilio tecnico almeno una volta. In aggiunta possono verificare risultati provvisori anche prima o durante lo scrutinio. In particolare, durante la fase di setup, possono anche ricorrere ai loro ausili tecnici per effettuare verifiche delle componenti di setup.
- Ausilio tecnico dei verificatori: per verificare la nota di conferma secondo il numero 2.6 i verificatori necessitano di un ausilio tecnico.

N. 2.2:



N. 2.3: in materia di requisiti posti al protocollo crittografico non viene fatta alcuna distinzione tra aggressori con diverse risorse o competenze tecniche: per la definizione del protocollo crittografico risulta irrilevante se un aggressore prende il controllo dei partecipanti al sistema mediante minacce, hackeraggio o ingegneria sociale. Costituisce invece un prerequisito il controllo acquisito dall'aggressore sui partecipanti al sistema non affidabili e sui canali di comunicazione. Il protocollo crittografico deve essere definito in modo tale che l'aggressore, nonostante gli attacchi riusciti su tali partecipanti al sistema e sui canali di comunicazione, non possa causare alcun danno. Ciò presuppone implicitamente che l'aggressore non sia in grado di distruggere gli elementi crittografici e la loro implementazione nel codice sorgente. I requisiti di cui ai numeri 2.13 e 2.14 e i requisiti concernenti la qualità dello sviluppo del software secondo i numeri 24 e 25 sono pensati per raggiungere questo obiettivo.

N. 2.3.2: l'aggressore può inserire messaggi attraverso canali non affidabili, ad esempio modificando o moltiplicando a proprio favore messaggi scambiati da altri attori.

Il numero 2.3.2 stabilisce le capacità di cui si presume disponga un aggressore («che cosa possono in ogni caso raggiungere gli aggressori»). Il numero 2.4 stabilisce in che misura tali capacità possono essere considerate limitate («che cosa non possono necessariamente raggiungere gli aggressori»).

N. 2.4: partecipanti al sistema e canali di comunicazione affidabili sono considerati protetti contro gli aggressori. Quanto meno gli elementi sono considerati affidabili, tanto più estesa deve essere la protezione del protocollo crittografico (cfr. commento introduttivo al n. 2). Il numero 2.9 stabilisce quali partecipanti al sistema e canali di comunicazione vanno considerati affidabili nell'ottica dei requisiti di cui ai numeri 2.5–2.8.

In linea di principio è auspicabile che partecipanti al sistema e canali di comunicazione siano considerati non affidabili anche quando, secondo il numero 2.9, questo non sarebbe necessario. Questa possibilità è tuttavia limitata. Ad esempio non sarebbe possibile rilevare manipolazioni secondo il numero 2.6 se tutti i verificatori non fossero affidabili e in tal modo operassero secondo le istruzioni dell'aggressore. Possibi-

lità per rafforzare ulteriormente la verificabilità indebolendo le ipotesi sull'affidabilità devono essere ricercate in collaborazione con il mondo scientifico sulla base dell'elenco di misure di Confederazione e Cantoni[11] e i sistemi devono essere adeguati di conseguenza.

I requisiti posti all'esercizio delle componenti affidabili sono illustrati nel numero 3.

Per i canali affidabili si deve partire dal presupposto che i messaggi tramessi attraverso di loro non siano manipolabili. In tal modo il destinatario del messaggio può fare affidamento sul fatto che il mittente corrisponde al partecipante al sistema specificato dalla definizione del canale.

N. 2.5: le note di conferma possono essere efficaci solo se gli aventi diritto di voto le esaminano effettivamente e, in caso di dubbio, si rivolgono all'autorità competente. In quale misura lo facciano e quali provvedimenti potrebbero contribuire a garantire che gli aventi diritto di voto esaminino le note di conferma secondo le istruzioni potrebbero essere oggetto di ricerca e di un accompagnamento scientifico. Alcuni requisiti dell'OVE potrebbero contribuire a rendere le note di conferma uno strumento efficace: ad esempio, la suddivisione delle note di conferma in note di conferma parziali secondo i numeri 2.12.5-2.12.10 permette agli aventi diritto di voto, in caso di difficoltà al momento della verifica, di interrompere anticipatamente l'operazione di voto elettronico e di ricorrere al voto per corrispondenza o al voto di persona. A differenza delle note di conferma parziali iniziali, la verifica della nota di conferma parziale che conferma il voto definitivo deve essere particolarmente semplice da realizzare. Il requisito di cui al numero 8.8 mira a rendere più difficili gli attacchi di ingegneria sociale volti a impedire agli elettori di effettuare correttamente la verifica delle note di conferma. Inoltre, il numero 8 impone ulteriori requisiti per le informazioni e l'assistenza agli aventi diritto di voto. Gli attacchi di ingegneria sociale devono essere valutati nel quadro dell'analisi dei rischi di cui al numero 13.

Una nota di conferma corretta conferma agli aventi diritto di voto che almeno la componente di controllo, che secondo il numero 2.9.1 può essere considerata affidabile, ha registrato il voto come espresso conformemente al sistema. Mediante la verifica delle note di conferma secondo il numero 2.6, i verificatori stabiliscono che anche il voto è stato conteggiato correttamente e quindi conformemente alla nota di conferma di cui al numero 2.5 visualizzata dall'avente diritto di voto. Affinché la verifica della nota di conferma secondo il numero 2.6 avvenga correttamente, tutte le componenti di controllo devono aver registrato gli stessi voti come espressi conformemente al sistema. I casi in cui le componenti di controllo mostrano incoerenze a questo proposito devono essere anticipati secondo il numero 11.11 e la procedura da seguire va determinata in anticipo.

La disposizione non prescrive come interpretare i casi in cui le note di conferma sono visualizzate in modo scorretto o non vengono affatto visualizzate. In particolare, sarebbe ipoteticamente possibile per il gruppo delle componenti di controllo registrare un voto espresso conformemente al sistema anche se questo non è stato espresso conformemente al sistema. Il numero 2.6 impone però che tali voti siano selezionati per essere successivamente vagliati in modo da permettere ai verificatori di assicurarsi che l'aggressore non abbia inserito voti non espressi conformemente al sistema. Inoltre, secondo il numero 10, il sistema NA (non necessariamente il gruppo di componenti di controllo) deve rilevare comunque tali voti quando vengono espressi e non deve trattarli come se fossero voti espressi conformemente al sistema.

Per quanto riguarda la precisazione «... l'aggressore non ha espresso abusivamente a nome dell'avente diritto alcun voto successivamente registrato e conteggiato quale voto espresso conformemente al sistema»: durante lo scrutinio tale nota di conferma sarebbe solo parzialmente utile dato che l'aggressore avrebbe ancora tempo per esprimere un voto. Pertanto è sufficiente se gli elettori possono richiedere questa nota di conferma dopo lo scrutinio. Per motivi di efficienza, è sufficiente che il servizio competente del Cantone confermi all'avente diritto di voto che non è stato espresso alcun voto a suo nome. Per la verifica da parte del servizio competente, si applicano le ipotesi sul grado di fiducia di cui al numero 2.9.1; in questo quadro anche l'ausilio tecnico del verificatore può essere considerato affidabile. Inoltre, questo requisito va oltre il modello di fiducia nella misura in cui l'aggressore secondo il numero 2.8 non deve assolutamente poter accedere alle caratteristiche di autenticazione client. Per quanto riguarda il presente requisito, si deve supporre che l'aggressore abbia accesso ai dati di autenticazione client di alcuni aventi diritto di voto.

[11] Cfr. le misure A.5 e A.6 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

N. 2.6: un voto è considerato espresso conformemente al sistema soltanto se i dati di autenticazione client utilizzati a tale scopo corrispondono a dati di autenticazione lato server definiti nella fase di preparazione dello scrutinio e «attribuiti» a un avente diritto di voto. La nota di conferma deve perciò contenere la conferma che non sono state generate caratteristiche di autenticazione non attribuiti per esprimere i voti. A tale scopo, durante la preparazione dello scrutinio, alle componenti di controllo o ai verificatori devono essere stati consegnati dati pertinenti quale termine di paragone. I verificatori devono constatare che il numero delle caratteristiche di autenticazione corrisponde al numero (ufficiale) degli aventi diritto di voto ammessi. In questo caso le caratteristiche di autenticazione possono essere considerate come «attribuite» a un avente diritto di voto. In tal modo non è ancora assicurato che caratteristiche di autenticazione *client* di aventi diritto affidabili non siano state utilizzate abusivamente per esprimere un voto conforme al sistema. Secondo il numero 2.5 gli aventi diritto di voto devono però essere in grado di determinarlo.

N. 2.7.2: meno voti sono conteggiati in una circoscrizione di conteggio, maggiore è la probabilità che tutti i voti siano uguali. Se un aggressore ha accesso al risultato di una circoscrizione di conteggio con voti identici e riesce anche a scoprire l'identità dei votanti, potrebbe violare il segreto del voto senza ulteriori sforzi. Potrebbe anche apprendere come gli elettori non hanno votato. Questo accade sia con il voto convenzionale che con quello elettronico. In conformità con il voto convenzionale, la presente ordinanza non regola la dimensione minima delle circoscrizioni di conteggio.

Nelle circoscrizioni di conteggio più grandi gli attacchi sono più difficili. Tuttavia, si presume qui che un aggressore tenti di violare il segreto del voto in un modo simile. In primo luogo, esercitando il controllo sui partecipanti al sistema non affidabili, dovrebbe garantire che solo un piccolo numero di voti giunga al conteggio. Per esempio, potrebbe cercare di manipolare il sistema NA in modo che non inoltri la maggior parte dei voti alla componente di controllo dopo che sono stati espressi. Se l'attacco ha successo, dopo la chiusura (possibilmente anticipata) del canale di voto elettronico, verrebbero registrati soltanto i voti di votanti che sono sotto il controllo dell'aggressore oppure il cui segreto di voto questi sta cercando di violare. Sulla base dell'affidabilità di almeno una componente di controllo, si raccomanda ai Cantoni, tenendo conto del numero di voti registrati dalle componenti di controllo, di considerare se un attacco sembra possibile e se il segreto del voto potrebbe essere minacciato dal conteggio. I Cantoni decidono se i voti devono essere conteggiati. Sulla base della crescente esperienza con il voto elettronico, i Cantoni stabiliscono il numero massimo di voti che potrebbe suggerire l'ipotesi di un attacco.

N. 2.7.3: si può supporre che la manipolazione del software sul server non abbia alcun effetto sull'affidabilità della piattaforma utente durante la verifica.

La base di paragone per la verifica può anche essere pubblicata su una piattaforma esterna sicura e considerata affidabile se ci sono buone ragioni per farlo. In particolare, tale piattaforma e il corrispondente canale di comunicazione possono essere considerati affidabili rispettivamente secondo i numeri 2.9.3.2 e 2.10.2.

Le possibilità di proteggere le piattaforme utente dalle aggressioni sono molto più ridotte rispetto alle componenti in un ambiente protetto. Tuttavia la decisione di non garantire il segreto del voto e l'esclusione di risultati parziali anticipati attraverso il protocollo crittografico è stata presa in modo consapevole per tenere in considerazione anche l'aspetto legato alla facilità d'uso da parte degli utenti. Il protocollo dovrebbe però fornire una protezione quando i voti sono memorizzati a livello centrale. La designazione della piattaforma utente come «affidabile» indica che nello sviluppo e nell'analisi del protocollo crittografico non si deve tener conto di alcun attacco alla piattaforma utente (cfr. spiegazioni concernenti il n. 2).

N. 2.9.3: una conseguenza è che la chiave necessaria per decrittare i voti deve essere ripartita su quattro diverse componenti di controllo. Di queste, almeno una deve essere gestita dal Cantone (cfr. n. 3.1).

Una parte significativa degli aventi diritto di voto deve essere considerata non affidabile affinché il sistema NA possa apprendere, in collaborazione con un avente diritto di voto non affidabile, il contenuto di un voto espresso. A tal fine, si deve garantire che questo avente diritto di voto non possa far passare per proprio un voto crittato espresso, anche dopo un adattamento esterno, allo scopo di conoscere il contenuto della scheda mediante la nota di conferma ottenuta nell'ambito della verifica delle note di conferma di cui al numero 2.5. Con l'aiuto dei partecipanti al sistema non affidabili un aggressore potrebbe cercare di segnare i voti prima del conteggio e successivamente violare il segreto del voto sulla base dei voti decrittati. Dopo il conteggio i verificatori potrebbero scoprire che i voti non sono stati processati conformemente alla

loro registrazione, ma in forma segnata. A questo punto, però, il segreto del voto sarebbe già stato violato. Questa eventualità va impedita ricorrendo a un gruppo di componenti di controllo prima del conteggio il quale garantisca che nessun voto segnato sia processato. Per quanto riguarda la designazione di «affidabile» applicata alla piattaforma utente, si rimanda al commento concernente il numero 2.7.3 (secondo paragrafo).

N. 2.9.3.3: con questa disposizione nessun gestore privato del sistema ha i dati che sarebbero necessari per violare il segreto del voto o per rilevare risultati parziali anticipati.

N. 2.11.1: una conseguenza di questa disposizione è che una nota di conferma deve poter assumere almeno 1000 valori diversi (per un codice numerico, ad esempio, tutti i valori tra 000 e 999). La probabilità che un aggressore indovini esattamente una nota di conferma è precisamente dello 0,1 per cento. Raccogliendo informazioni sui partecipanti al sistema non affidabili e sui canali di comunicazione, l'aggressore potrebbe essere avvantaggiato nel senso che non dovrebbe più procedere completamente alla cieca per scoprire il codice, aumentando le sue probabilità di successo. In considerazione di questa possibilità un codice deve poter assumere a priori valori sufficienti affinché la probabilità non superi lo 0,1 per cento.

N. 2.11.3: si suppone ad esempio che la probabilità per l'aggressore di falsificare una nota di conferma sia dell'1 per cento. In questo caso le diverse operazioni di conteggio devono poter essere ripetute fino a far scendere questo valore al di sotto dell'1 per cento. Ripetendo più volte le operazioni di conteggio dovrebbe essere possibile ridurre la probabilità quanto necessario.

N. 2.12.4: con questa dichiarazione, il voto non è ancora espresso in modo definitivo. In primo luogo, il votante deve avere la possibilità di verificare la corretta trasmissione attraverso una prima nota di conferma parziale. In seguito, deve avere la possibilità di annullare il voto e di esprimere il voto attraverso un canale convenzionale.

N. 2.12.5: le note di conferma sono suddivise in note di conferma parziali per una questione di facilità d'uso e non per ottenere una maggiore validità.

Non è permesso fare effettuare una verifica ai votanti per ragioni puramente psicologiche se il risultato della verifica non ha alcuna rilevanza in relazione alla valutazione della manipolazione del voto.

N. 2.12.8: se, per adempiere i requisiti di cui al numero 2.5, sono impiegate due note di conferma parziali, la penultima nota di conferma parziale equivale alla prima. Inoltre, dal numero 2.8 si può dedurre che gli aventi diritto di voto devono inserire con la loro dichiarazione d'intenti secondo il numero 2.12.8 un elemento segreto che non è ancora stato inserito nella piattaforma utente. L'elemento segreto può anche essere inteso quale funzione di autenticazione lato client.

N. 2.12.11: le componenti di setup e le componenti di stampa sono fondamentalmente previste per la preparazione dello scrutinio. Il loro uso in un momento successivo non è però vietato. Tuttavia non dovrebbe essere possibile processare voti o altri dati che si presentano solo durante lo scrutinio, presupponendo che queste componenti siano affidabili. Se utilizzate per processare i dati, tali componenti devono essere considerate non affidabili.

N. 2.14.1: nei casi in cui si applica il numero 2.9.3.3, come conseguenza dell'esclusione di cui al numero 2.7.2 nelle prove sull'adempimento del numero 2.7 si possono fare ipotesi diverse rispetto ai numeri 2.9.3.1 e 2.9.3.2. Per esempio, sarebbe lecito ipotizzare che una componente di controllo registri correttamente e successivamente non cancelli un numero sufficiente di voti di aventi diritto di voto affidabili come trasmesso dalla piattaforma utente affidabile. In alternativa, sarebbe ammissibile assumere che il segreto del voto non sia messo in pericolo se non tutti i voti espressi ma un sottoinsieme qualunque viene conteggiato una volta.

N. 3 Requisiti posti alle componenti affidabili secondo il numero 2 e al loro esercizio

Qui sono posti i requisiti alle componenti che, conformemente al protocollo crittografico, sono considerate affidabili quando almeno uno dei requisiti secondo i numeri 2.5–2.8 è soddisfatto. Le componenti interessate sono le seguenti:

- componenti di *setup*
- componenti di stampa

- componenti di controllo
- ausili tecnici per i verificatori

N. 3.1: rientrano nell'esercizio la configurazione (sistema operativo, ambiente di esecuzione, software per il voto elettronico), la verifica della correttezza dei file con il software per il voto elettronico, l'aggiornamento, la configurazione e la messa in sicurezza delle rispettive componenti. Cfr. anche il commento al numero 2.9.3.

N. 3.2: quale base per la scelta di valori casuali (in inglese «*seed*»), si deve aggregare almeno abbastanza entropia in modo che le componenti di base crittografiche secondo il numero 15.4 siano efficaci. Per ottenere questo effetto è opportuno aggregare valori casuali da diverse componenti indipendenti. In ogni caso, devono essere utilizzate funzioni e basi generalmente riconosciute come affidabili. Se necessario, occorre provvedere affinché ci siano le condizioni necessarie. Tra le condizioni vi può essere quella che un sistema operativo non calcoli un valore casuale fino a quando le fonti utilizzate (che possono includere, per esempio, il movimento del puntatore del mouse) non abbiano dato contributi sufficienti all'entropia.

N. 3.4: l'organizzazione concreta e l'impostazione dell'impiego dei verificatori è disciplinata a livello cantonale. Cfr. anche il commento all'articolo 27*m* cpv. 2 ODP.

N. 3.6: il processo di verifica deve essere osservabile, ovvero i verificatori devono essere in grado di comprendere per quanto possibile il significato e i risultati delle differenti tappe. A tal fine, devono poter attestare l'esecuzione corretta delle tappe e dei risultati dei test, ad esempio recandosi sul luogo dell'esecuzione. Per quanto riguarda l'installazione del software, si osservi il numero 24.3.

N. 3.7: si intendono non solo il software per il voto elettronico ma anche il software per l'infrastruttura, come i sistemi operativi. Occorre accertarsi che il software provenga da una fonte ufficiale e affidabile.

N. 3.14: a differenza di una forma più debole del principio del doppio controllo, si deve garantire che una persona non possa accedere a dati critici senza che un'altra persona se ne accorga. Non è quindi sufficiente limitare il principio del doppio controllo all'esecuzione delle fasi del processo. Conformemente a una rigorosa applicazione del principio del doppio controllo, la salvaguardia sicura dei dati critici potrebbe consistere nel salvare i dati criptati su un supporto dati e conservare il supporto dati in una cassaforte. Una delle due persone conosce il codice di accesso alla cassaforte e l'altra ha la chiave per decifrare i dati.

N. 3.15: è sufficiente utilizzare lo stesso software per tutte le componenti di controllo. In futuro, per le singole componenti di controllo dovrebbe essere utilizzato un software indipendente dal produttore, basato sull'elenco di misure di Confederazione e Cantoni[12].

N. 3.18: un software indipendente dal produttore per l'ausilio tecnico dei verificatori sarà utilizzato in futuro sulla base dell'elenco di misure di Confederazione e Cantoni[13].

N. 4 Procedura di voto

N. 4.9: si tratta di una disposizione che autorizza il Cantone a offrire la funzionalità corrispondente. Il Cantone non è obbligato a farlo.

N. 4.10: più precisamente, in questo caso la validità delle note di conferma può essere fatta dipendere dall'affidabilità della piattaforma utente. Ciò consente ad esempio la scansione del riferimento di verifica prima di esprimere il voto. Queste facilitazioni possono essere concesse solo a un piccolo gruppo di aventi diritto di voto i quali senza tale agevolazione non sarebbero in grado di interpretare la nota di conferma. Tutti gli altri devono essere in linea di massima esortati a verificare le note di conferma secondo la procedura prevista.

N. 4.11: gli aventi diritto di voto sono tenuti a segnalare alle autorità cantonali competenti se le note di conferma sono visualizzate in modo errato o se hanno dubbi al riguardo. Esprimere il proprio voto di

[12] Cfr. la misura A.4 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

[13] Cfr. la misura A.4 del rapporto finale del CD VE del 30 novembre 2020; consultabile sotto www.bk.admin.ch > Diritti politici > Voto elettronico > Rapporti e studi.

persona o per corrispondenza resta possibile fintantoché non si ha già votato elettronicamente. Per verificare se l'avente diritto di voto può ancora avvalersi del voto di persona o per corrispondenza i Cantoni possono ricorrere alla funzione descritta al numero 11.6.

N. 4.12: la conferma dell'espressione definitiva del voto secondo il numero 2.12.8 deve essere effettuata utilizzando un elemento segreto, non ancora inserito nella piattaforma utente. Al posto di tale elemento segreto non si esclude di ricorrere a un e-ID. Tale scelta dovrebbe essere basata su una valutazione dei rischi. Un e-ID non può tuttavia sostituire la consegna per posta del riferimento di verifica. Per il momento resterà necessario consegnare il materiale di voto per posta.

Inoltre la disposizione secondo cui l'ammissibilità del ricorso a un e-ID deve essere esaminata sulla base di una valutazione dei rischi si applica anche se questo e-ID è rilasciato o riconosciuto dallo Stato.

N. 7 Requisiti posti alle tipografie

I requisiti posti alle tipografie non saranno più disciplinati in un catalogo distinto ma direttamente nell'allegato dell'OVE. Queste disposizioni si applicano segnatamente in aggiunta a quelle di cui al numero 3.

N. 7.4: ad esempio i supporti di dati e l'elemento segreto per la decrittazione devono essere conservati separatamente in un luogo sicuro (ad es. in una cassaforte). La persona in possesso dell'elemento segreto per decrittare i dati non deve poter aprire la cassaforte senza poter essere tracciata. La decrittazione e l'elaborazione dei dati così come il processo di stampa sono eseguiti secondo il principio del doppio controllo. Non deve essere possibile far figurare su una componente dati non crittati senza che almeno due persone la sorvegliano e, se necessario, informino su un eventuale abuso.

Se durante l'elaborazione di dati critici il principio del doppio controllo non può essere implementato senza soluzione di continuità, ad esempio a causa di un'interruzione prolungata, i dati devono essere distrutti.

N. 7.6: se ci sono buoni motivi la distruzione dei dati può essere rimandata al più tardi fino a quando i requisiti legali relativi alla conservazione e alla tracciabilità sono soddisfatti.

N. 8 Informazioni e istruzioni

N. 8.8: a quanto stabilito da questa disposizione si deve in particolare prestare attenzione anche quando la prima nota di conferma parziale secondo il numero 2.12.5 è stata visualizzata in modo errato e l'avente diritto al voto ha di conseguenza interrotto il processo di voto.

N. 8.9: l'obiettivo di questa disposizione è contrastare i casi in cui terzi esprimono abusivamente un voto utilizzando materiale di voto appartenente ad altri. In questo contesto, si deve tener conto che i titolari del materiale di voto non possono necessariamente riconoscere un voto abusivo senza consultare il sistema come prevede il numero 2.5 (secondo trattino). Inoltre, bisogna tener conto che anche dopo la visualizzazione della prima nota di conferma parziale secondo il numero 2.12.5 può essere ancora possibile esprimere un voto.

N. 8.11: gli aventi diritto di voto devono conoscere la corretta procedura di voto per essere protetti dagli attacchi di ingegneria sociale. Inviando le istruzioni per posta e consigliando agli aventi diritto di voto, in caso di dubbio, di attenersi a queste istruzioni e, se necessario, di contattare il servizio cantonale competente, le autorità riducono il margine d'azione per gli attacchi di ingegneria sociale. L'efficacia di questa procedura così come eventuali procedure alternative per guidare gli aventi diritto di voto potrebbero essere oggetto di progetti di ricerca e di accompagnamento scientifico.

N. 10 Controllo della conformità e deposito di voti espressi in modo definitivo

Per il conteggio possono essere depositati soltanto voti espressi conformemente al sistema. Questo controllo può essere effettuato anche con una componente non affidabile secondo il numero 2.

La nozione di «urna elettronica» indica l'area dati in cui sono memorizzati i voti destinati ad essere conteggiati. L'urna elettronica può essere implementata dalle componenti di controllo di cui al numero 2. In alternativa, è possibile prevedere un'area dati supplementare dove memorizzare i dati. In questo caso, ai sensi del numero 2.4 l'urna elettronica deve in ogni caso essere considerata non affidabile.

N. 11 Spoglio dei voti depositati nell'urna elettronica

N. 11.1: la decrittazione secondo il numero 11.2 deve avvenire la domenica della votazione. Decrittazioni a monte, effettuate presso il gestore del sistema, possono iniziare non appena il canale di voto elettronico è stato chiuso. L'efficacia della decrittazione deve rimanere alta nonostante le procedure a monte.

N. 11.2: se è utilizzato il sistema di un altro Cantone la decrittazione e lo spoglio possono avvenire anche nel Cantone che fornisce il sistema.

N. 11.6: usando come unica base di confronto i soli voti espressi elettronicamente non è possibile determinare se un avente diritto di voto che ha espresso il proprio voto di persona o per corrispondenza abbia già votato (due o più volte). Nonostante questo la possibilità di cui al numero 11.6 rientra nel campo di applicazione dell'OVE. Non è tuttavia necessario specificare tale possibilità con riferimento alle ipotesi sul grado di fiducia secondo il numero 2.

N. 11.7: sul posto devono per principio essere presenti verificatori. Ad altri verificatori può inoltre essere concessa la possibilità di seguire le procedure, per esempio, tramite un collegamento in diretta.

N. 12 Dati confidenziali

N. 12.7: la Confederazione non disciplina la dimensione minima delle circoscrizioni di conteggio – e quindi, in particolare, neppure dei circondari elettorali (cfr. commento al n. 2.7.2). Nella misura in cui è necessario per preservare il segreto del voto, nel caso di piccoli circondari elettorali i risultati dovrebbero essere trattati in modo confidenziale. Nei casi in cui i circondari elettorali sono suddivisi in singole circoscrizioni di conteggio, questa condizione si applica per analogia.

N. 12.8: in particolare per le componenti del sistema la cui affidabilità è decisiva per salvaguardare il segreto del voto secondo il numero 2.9.3, si deve garantire che i dati siano stati cancellati definitivamente, senza possibilità di recupero.

N. 13 Minacce

Gli obiettivi di sicurezza (cfr. art. 4 cpv. 3 OVE) non possono essere raggiunti con assoluta certezza, ma si possono in ogni caso identificare i rischi per la sicurezza. Sulla base di una metodica valutazione dei rischi (art. 4 cpv. 1 OVE) occorre fornire la prova che eventuali rischi per la sicurezza sono da considerarsi sufficientemente bassi.

È possibile identificare un rischio attraverso le minacce e i punti deboli del sistema. Un rischio insorge quando un punto debole di tale sistema può essere sfruttato mediante una minaccia, mettendo potenzialmente in dubbio l'adempimento di uno o più obiettivi di sicurezza. Per ridurre i rischi si attuano misure di sicurezza che devono adempiere i requisiti di sicurezza a livello di infrastruttura, funzionalità ed esercizio in modo da ridurre a sufficienza i rischi identificati.

L'elenco delle minacce è stato adeguato in base alle conoscenze emerse negli ultimi anni e all'uso di sistemi completamente verificabili. Per chiarire i vari scenari è stata introdotta una nuova denominazione degli attori delle minacce con la relativa definizione.

N. 13.12: il protocollo chiede che gli aventi diritto di voto esaminino le note di conferma secondo il numero 2.5. Secondo la citata disposizione deve essere valutato il rischio di alterazione delle informazioni fornite dal Cantone da parte di un aggressore esterno al fine di indurre gli aventi diritto di voto a non attenersi alle fasi previste per la verifica. Concretamente si tratta di non prendere in considerazione informazioni false che potrebbero essere diffuse sui social network.

N. 13.13, 13.14 e 13.15: per mezzo elettronico si intende qualsiasi mezzo che permette di accedere a informazioni importanti senza che l'aggressore debba essere fisicamente presente in loco (ad es. malware).

È invece considerato un mezzo fisico qualsiasi mezzo che permette l'accesso a informazioni importanti da parte dell'aggressore a condizione che quest'ultimo sia sul posto.

L’ingegneria sociale corrisponde a una procedura attraverso la quale un aggressore ottiene l’accesso a informazioni importanti ingannando una persona al fine di indurla a fornire lei stessa le informazioni desiderate oppure a concedere l’accesso a un terzo attraverso mezzi fisici o elettronici.

N. 13.16, 13.17 e 13.18: il protocollo crittografico definisce determinati parametri, algoritmi e procedure. Le minacce qui menzionate sfrutterebbero una vulnerabilità in uno o più di uno di questi elementi.

N. 14 Constatazione e notifica di eventi e debolezze inerenti alla sicurezza; gestione di eventi e miglioramenti inerenti alla sicurezza

I sistemi di voto elettronico devono consentire di individuare ed esaminare in modo efficace gli incidenti, quali presunte manipolazioni di voto o attacchi al sistema. Il contenuto e la portata dei protocolli del sistema devono essere definiti con questo scopo, garantendo nel contempo il segreto del voto.

Inoltre deve essere definito un processo costante di miglioramento in merito all’individuazione e all’esame degli incidenti. A tal fine occorrerà provvedere a:

- un dialogo aperto fra Confederazione, Cantoni e gestore del sistema;
- analisi regolari sull’idoneità delle basi del monitoraggio e dell’esame degli incidenti. Gli scenari definiti nella convenzione di crisi sono considerati al fine di queste analisi. La partecipazione a queste analisi di esperti in materia di informatica forense permette di apportare miglioramenti più efficaci.
- migliorare gli strumenti e i processi tenendo conto degli elementi risultanti dalle analisi.

L'aspetto tecnico di questi requisiti è diretto principalmente al gestore del sistema. L'organo responsabile a livello cantonale deve comprendere il contenuto del protocollo del sistema ed essere in grado di rispondere a un messaggio trasmesso dal suo gestore del sistema.

N. 14.2: i processi di audit, di identificazione e di autenticazione sono particolarmente sensibili e richiedono un controllo speciale, sia nella parte del sistema gestita dal Cantone sia in quella gestita dal gestore del sistema. L’identificazione corrisponde al processo di identificazione di una persona, ad esempio mediante nome utente o smartcard. L’autenticazione è invece il processo attraverso il quale il sistema rilascia l’autorizzazione d’accesso, ad esempio mediante la verifica di una password.

N. 14.7: l’obiettivo è quello di determinare che i voti siano processati e conteggiati correttamente. A tal fine, i voti di controllo sono processati secondo le stesse procedure impiegate per i voti espressi conformemente al sistema. I voti di controllo non devono essere inclusi nel risultato finale come voti espressi conformemente al sistema.

N. 14.9: questa disposizione non riguarda necessariamente solo il sistema online. Ad essere interessate sono anche le componenti nei lavori preparatori preliminari o successivi agli scrutini.

N. 15 Utilizzo di misure crittografiche e amministrazione delle chiavi

N. 15.3: la crittografia a livello del software, la cui necessità si evince dal numero 2, non è sufficiente a soddisfare questo requisito.

N. 16 Scambio di informazioni fisico ed elettronico sicuro

N. 16.2: il sistema deve essere separato da tutte le altre attività a livello logico o fisico. Tuttavia, alcune componenti dell’infrastruttura (ad esempio monitoraggio, *firewall*) possono essere condivise con altre attività se questo non aumenta significativamente i rischi del sistema e fornisce un vantaggio importante.

N. 17 Test del sistema

N. 17.2: le interfacce sono gli elementi che permettono al software di scambiare informazioni con il suo ambiente. Può trattarsi di interfacce grafiche, linee di comando o interfacce tecniche (API).

N. 17.3: per questo requisito sono considerati due livelli di struttura del software:

- un modulo è il livello più basso e costituisce un raggruppamento di classi nel codice sorgente che mirano a un obiettivo ben definito;
- un sottosistema è un insieme di moduli che copre una funzionalità del sistema, ad esempio l'amministrazione di una votazione, la creazione di una carta di legittimazione di voto o la registrazione del voto espresso.

N. 22 Gestione della comunicazione e dell'esercizio

N. 22.3: la verifica del corretto funzionamento della sicurezza dei dati è effettuata almeno con un test di recupero dei dati. Tale test può essere integrato da altri controlli finalizzati a migliorare costantemente i processi di sicurezza dei dati.

N. 24 Sviluppo e manutenzione di sistemi di informazione

La qualità dei sistemi di voto elettronico deve essere garantita durante l'intero processo di sviluppo. Al fine di rafforzare la garanzia della qualità i requisiti sono stati specificati perseguendo gli obiettivi seguenti:

- permettere la tracciabilità e la verifica delle modifiche apportate al sistema;
- garantire in qualsiasi momento e in entrambe le direzioni la tracciabilità tra i singoli elementi della documentazione (protocollo, specifica, architettura, ecc.) e il codice sorgente;
- far confluire i risultati delle procedure di verifica nei lavori di sviluppo;
- garantire e mantenere la conformità ai requisiti legali per tutto il ciclo di vita.

In particolare, i requisiti del livello *common criteria* EAL 4, che fino ad ora si applicavano alle componenti di controllo, sono estesi all'intero sistema. Inoltre sono stati completati con requisiti dei *common criteria* concernenti EAL 4 quando questa integrazione poteva contribuire in modo significativo agli obiettivi di sicurezza ed era in linea con gli obiettivi succitati.

N. 24.1: le funzioni di sicurezza sono di fondamentale importanza per il software. Devono quindi essere trattate con particolare attenzione ed essere tracciabili in tutte le fasi del processo di sviluppo. È importante assicurarsi che tutte le funzioni di sicurezza previste nella progettazione del software siano presenti a tutti i livelli fino al codice sorgente. La nozione di «codice sorgente» include qui anche qualsiasi libreria esterna.

Gli strumenti di sviluppo qui considerati sono gli strumenti importanti per la sicurezza dello sviluppo del software. Tra questi rientrano ambienti di sviluppo integrato (*integrated development environment, IDE*), strumenti di costruzione (*build tools*) e strumenti di gestione della configurazione. Rientrano in questa categoria anche le opzioni di configurazione che possono avere un impatto sulla sicurezza dello sviluppo.

Come nel numero 17.2, per interfacce si intendono quegli elementi che permettono al software di scambiare informazioni con il suo ambiente. Può trattarsi di interfacce grafiche, linee di comando o interfacce di programmazione (API).

Un elenco di configurazione è un insieme unificato di elementi di configurazione che rappresenta lo stato del software e della sua documentazione in un particolare momento. Idealmente, permette di ricostruire una versione precedente del software.

N. 24.3: deve essere garantito un corretto approntamento del sistema a partire dal codice sorgente fino alla sua installazione in produzione (*build and deployment*). A tale scopo il gestore del sistema deve impiegare un metodo comprovato e tracciabile di *build and deployment* per raggiungere i seguenti obiettivi:

- il metodo *build and deployment* consente di garantire che il software impiegato corrisponda alla versione pubblicata, verificata e autorizzata;
- oltre a questa tracciabilità, il metodo *build and deployment* dovrebbe consentire di prevenire il più possibile la manipolazione delle componenti del sistema;

- occorre evitare che con gli strumenti di sviluppo e le biblioteche utilizzate si introducano punti vulnerabili nel software rendendo così il sistema vulnerabile agli attacchi.

A questo scopo sono stati introdotti nuovi requisiti, basati sulle linee guida dello stato federale americano del Colorado per l'uso dei sistemi di voto elettronici[14], sulla documentazione Trusted Build pubblicata da GitHub[15] e sulla documentazione Reproducible Builds[16] dell'omonimo progetto.

N. 24.3.3: per quanto riguarda «la prova che tutte le firme crittografiche delle dipendenze sono state verificate rispetto a un riferimento comprovato, pubblico e affidabile»: un riferimento affidabile potrebbe per esempio essere il *Maven Central Repository*.

N. 24.4: sono considerate utenti tutte le persone che, in un modo o nell'altro, entrano in contatto con il software. Sono ad esempio utenti gli impiegati cantonali, gli aventi diritto di voto, coloro che effettuano i test e, in definitiva, chiunque abbia un interesse nel sistema.

Affinché lo sviluppatore gestisca le segnalazioni di difetti in modo appropriato e in questo contesto comunichi in modo efficace, è importante che gli utenti sappiano come trasmettergli le segnalazioni di difetti e come registrarsi per ricevere informazioni appropriate.

Per contribuire a migliorare la sicurezza di un sistema bisogna allestire un elenco il più completo possibile delle vulnerabilità sospette e dei correttivi da attuare sistematicamente. Questi requisiti sono complementari alla divulgazione del codice sorgente (art. 11–12 OVE) e al programma *bug bounty* (art. 13 OVE).

N. 25 Qualità del codice sorgente e della documentazione

La qualità del codice sorgente e della documentazione è fondamentale per la sicurezza del voto elettronico. Le basi legali attuali definiscono i requisiti a tal proposito. Le descrizioni hanno però carattere piuttosto generale: si pensi ad esempio all'obbligo di preparare e documentare il codice sorgente conformemente alle migliori prassi e all'attuazione di determinati punti di *common criteria*. I criteri di qualità esistenti sono stati pertanto precisati nel presente revisione. Grazie a criteri chiari si vuole garantire un'elevata qualità dei sistemi di voto elettronico che a sua volta andrà a beneficio della sicurezza agevolando le verifiche di tutte le parti interessate e del pubblico. Per definire questi criteri di qualità è stato creato un modello di qualità per i sistemi di voto elettronico. Questo modello è basato sulla norma ISO 25010 e sul modello di qualità di McCall[17]. I criteri sono stati selezionati in base al loro contributo agli obiettivi di sicurezza e qualità definiti.

N. 25.7.3: il portale di voto elettronico deve in linea di principio essere privo di barriere e rispettare la norma di accessibilità eCH-0059. I contenuti della norma sono obbligatori, ad eccezione dei requisiti posti a forme di comunicazione alternative (cfr. cap. 2.4 della norma). Al di là delle condizioni concernenti il voto per corrispondenza o all'urna, non sono previsti requisiti su come mettere a disposizione informazioni in un linguaggio semplice e nella lingua dei segni, in particolare sull'allestimento di modelli, ad esempio per le spiegazioni di voto o le istruzioni di voto. La prova che il portale di voto elettronico è conforme ai requisiti della norma eCH-0059 include un certificato o un rapporto d'esame da parte di un servizio specializzato.

N. 25.13.2: l'obiettivo di questo requisito è di impedire comportamenti inaspettati per tutte le parti del software e per tutti i valori possibili. A tal scopo, da ogni serie di valori che portano a risultati diversi deve essere testato almeno un valore. All'interno di un insieme di valori, non tutti i valori devono essere testati. Anche le situazioni di errore devono essere testate.

---

[14] Colorado Election Rules [8 CCR 1505-1] Rule 1. Definitions, 2020 e Colorado Voting Systems Trusted Build Procedures, 2020

[15] GitHub How to: Trusted builds, 2017

[16] https://reproducible-builds.org/

[17] FACTORS IN SOFTWARE QUALITY - Vol. 1: Concept and Definitions of Software Quality - Jim A. McCall, Paul K. Richards, Gene F. Walters (1977)

N. 26 Criteri di verifica dei sistemi e del loro esercizio

Per garantire l'efficacia e la credibilità delle verifiche sono state adeguate le competenze. La suddivisione dei compiti fra la Confederazione e i Cantoni sarà quindi modificata in modo tale che la Confederazione assuma maggiori responsabilità e un ruolo più diretto nella verifica dei sistemi.

Alla Confederazione compete la verifica del rispetto dei requisiti inerenti al sistema e dei relativi sottoprocessi. Questo non da ultimo per garantire che i risultati della revisione vengano integrati in modo mirato nelle successive fasi di test. Le verifiche dovranno essere commissionate a esperti indipendenti.

Il Cantone / il gestore del sistema rimarrà responsabile per le verifiche in relazione all'esercizio del sistema nei suoi centri di calcolo (certificazione ISO 27001).

Si rinuncia a una certificazione più estesa da parte di servizi a loro volta accreditati dal Servizio di accreditamento svizzero (SAS).