

06.056

Rapporto sui progetti pilota in materia di voto elettronico

del 31 maggio 2006

Onorevoli presidenti e consiglieri,

vi sottoponiamo il rapporto sui progetti pilota in materia di voto elettronico, proponendovi di prenderne atto.

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

31 maggio 2006

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Moritz Leuenberger

La cancelliera della Confederazione, Annemarie Huber-Hotz

Compendio

Contenuto

Il presente rapporto fornisce un bilancio dei progetti pilota realizzati negli anni 2001–2005 con i Cantoni di Ginevra, Neuchâtel e Zurigo e propone l'introduzione del voto elettronico in modo graduale e con la dovuta consapevolezza dei rischi che vi sono connessi.

Situazione iniziale

Con il presente rapporto il Consiglio federale conclude la valutazione delle opportunità, dei rischi e della fattibilità del voto elettronico in Svizzera, avviata in seguito a interventi parlamentari degli anni 1999 e 2000. I vasti lavori di analisi delle prove pilota svolte negli anni 2004 e 2005 in tre Cantoni fungono da base di decisione e di discussione sulla procedura da seguire.

Che cosa significa voto elettronico?

Nel presente rapporto s'intende per voto elettronico la possibilità di votare ed eleggere per via elettronica e di firmare elettronicamente referendum, iniziative e proposte di elezione nel Consiglio nazionale.

Le opportunità e i rischi del voto elettronico

Il voto elettronico consente di garantire alle generazioni future la partecipazione democratica anche se cambiano le condizioni di vita, assicurando così la legittimazione di decisioni politiche ampiamente approvate dal popolo; permette inoltre di semplificare ulteriormente il voto in una società sempre più mobile, in cui aumentano costantemente gli Svizzeri all'estero con diritto di voto. Grazie al voto elettronico, le persone ipovedenti possono votare in segreto senza ricorrere all'aiuto di terzi. Infine, con il voto elettronico, la Svizzera può far conoscere a livello internazionale le sue istituzioni di democrazia diretta e affermarsi con un ulteriore moderno servizio in un mercato molto promettente.

In questo ambito si corrono però anche rischi: il voto elettronico richiede l'adozione di misure complesse a livello organizzativo, tecnico e giuridico; il divario digitale tra le persone con accesso a Internet e quelle che ne sono prive rischia di accentuare le disparità per quanto riguarda la partecipazione alla vita politica; nuovi rischi tecnici di abusi esigono che le misure di sicurezza siano costantemente controllate e aggiornate; ogni abuso, reale o presunto, e ogni disfunzione tecnica possono creare insicurezza e minare la fiducia degli aventi diritto di voto nella democrazia diretta. Il voto per corrispondenza viene utilizzato come valore di riferimento per la valutazione dei rischi del voto elettronico.

Utilità e costi del voto elettronico

Il Consiglio federale ritiene ampiamente dimostrata l'utilità del voto elettronico. Il voto elettronico permette di sostenere in modo efficace e duraturo i diritti politici dell'elettorato. Con il voto elettronico si possono creare le condizioni per mantenere a lungo, in una società che si modernizza, le istituzioni della democrazia diretta della Svizzera. Le possibilità di partecipazione politica devono stare al passo con le mutevoli abitudini di vita dei cittadini. Non vi è motivo di rinunciare a continuare le prove pilota avviate con successo né di ampliarle con fretta eccessiva. Il Consiglio federale intende offrire ai Cantoni la possibilità di introdurre il voto elettronico gradualmente.

In caso di introduzione capillare del voto elettronico in Svizzera, i costi per un periodo di dieci anni sono stimati a 65,76 milioni di franchi per un sistema unico per tutti i Cantoni, a 92,16 milioni di franchi per sei sistemi diversi e fino a 400 milioni di franchi per soluzioni cantonali individuali. A questi costi si contrappone un potenziale di risparmio di 27,86 milioni di franchi nell'ambito del voto per corrispondenza. Di conseguenza, l'introduzione del voto elettronico in tutta la Svizzera provocherebbe costi netti minimi di 37,90 e massimi di 400 milioni di franchi, per la maggior parte a carico dei Comuni e dei Cantoni; la Confederazione dovrebbe sopportare, oltre alle spese iniziali già pagate, solo circa 350 000 franchi all'anno per il coordinamento.

Ulteriore procedura

Secondo il Consiglio federale, si devono creare a livello di Confederazione basi giuridiche che consentano di introdurre il voto elettronico nei Cantoni seguendo una suddivisione regolare in tappe e processi di controllo coordinati dalla Confederazione. È molto importante che i rischi siano calcolabili. Spetta ai Cantoni e ai Comuni decidere se, come e quando introdurre il voto elettronico per votazioni cantonali e comunali dato che sarebbero loro a dover sostenere la maggior parte dei costi. Nell'ambito delle sue autorizzazioni per le votazioni federali, il Consiglio federale provvederà a fare in modo che nel corso della prossima legislatura non siano chiamati a partecipare a prove pilota del voto elettronico aventi luogo contemporaneamente più del 10 per cento degli aventi diritto di voto a livello federale. Inoltre, in caso di referendum obbligatori, per i quali è determinante anche la maggioranza dei Cantoni, non sarà ammesso al voto elettronico più del 20 per cento dei corpi elettorali cantonali interessati.

La collaborazione innovativa ed efficiente dei Cantoni di Ginevra, Neuchâtel e Zurigo tra loro e con la Confederazione ha portato alla realizzazione di tre sistemi di voto elettronico che si sono rivelati validi nel corso di diverse prove pilota a livello comunale, cantonale e federale. Questi sistemi sono ora a disposizione degli altri Cantoni: spetta a loro scegliere quello più adatto alle proprie esigenze.

Indice

| | |
|---|-------------|
| Compendio | 5016 |
| 1 Situazione iniziale | 5021 |
| 1.1 Che cos'è il voto elettronico? | 5021 |
| 1.2 Mandato del Parlamento | 5022 |
| 2 Condizioni per lo svolgimento di prove pilota | 5023 |
| 2.1 Basi legali per lo svolgimento di prove pilota | 5023 |
| 2.2 Convenzioni con i Cantoni pilota | 5023 |
| 2.3 Procedura di autorizzazione di prove pilota da parte del Consiglio federale | 5024 |
| 2.4 Armonizzazione dei cataloghi elettorali e identificatore delle persone | 5025 |
| 2.5 Esigenze relative al diritto in materia di protezione dei dati | 5026 |
| 3 Criteri di valutazione | 5026 |
| 3.1 Utilità e ripercussioni sulla democrazia diretta | 5026 |
| 3.2 Protezione contro i rischi e gli abusi | 5027 |
| 3.3 Economicità e fattibilità politica | 5029 |
| 4 Prove pilota negli anni 2004 e 2005 | 5030 |
| 4.1 Il progetto pilota del Cantone di Ginevra | 5030 |
| 4.1.1 Condizioni quadro | 5030 |
| 4.1.2 Basi legali e condizioni cantonali | 5030 |
| 4.1.3 Soluzione e realizzazione | 5031 |
| 4.1.4 Prove pilota e lavori collaterali | 5033 |
| 4.1.4.1 Lavori collaterali | 5034 |
| 4.2 Il progetto pilota del Cantone di Neuchâtel | 5035 |
| 4.2.1 Condizioni quadro | 5035 |
| 4.2.2 Basi legali e condizioni cantonali | 5035 |
| 4.2.3 Soluzione e realizzazione | 5036 |
| 4.2.3.1 Voto elettronico integrato nel Guichet Unique | 5036 |
| 4.2.3.2 Nuova organizzazione degli scrutini | 5037 |
| 4.2.3.3 Processo di voto elettronico | 5038 |
| 4.2.4 Prove pilota e lavori collaterali | 5038 |
| 4.2.4.1 Prove pilota e audit di sicurezza | 5038 |
| 4.2.4.2 Lavori collaterali | 5040 |
| 4.3 Il progetto pilota del Cantone di Zurigo | 5041 |
| 4.3.1 Condizioni quadro | 5041 |
| 4.3.2 Basi legali e condizioni cantonali | 5041 |
| 4.3.3 Soluzione e realizzazione | 5041 |
| 4.3.3.1 Una votazione con il voto elettronico | 5043 |
| 4.3.4 Prove pilota e lavori collaterali | 5044 |
| 4.3.4.1 Lavori collaterali | 5046 |
| 4.4 Progetti di altri Stati | 5046 |
| 4.4.1 Consiglio d'Europa e OSCE | 5047 |
| 4.5 Conclusione | 5048 |

| | |
|---|-------------|
| 5 Valutazione delle prove pilota | 5050 |
| 5.1 Utilità e ripercussioni sulla democrazia diretta | 5050 |
| 5.1.1 Studio sul potenziale 2003–2004 | 5051 |
| 5.1.2 Sondaggi nell’ambito delle prove pilota cantonali in occasione di votazioni popolari federali | 5053 |
| 5.1.2.1 Cantone di Ginevra | 5053 |
| 5.1.2.2 Cantone di Neuchâtel | 5055 |
| 5.1.2.3 Cantone di Zurigo | 5056 |
| 5.1.2.4 Inchieste di terzi | 5056 |
| 5.1.3 Le facilitazioni portano una maggiore partecipazione al voto? | 5057 |
| 5.1.4 Conclusione | 5059 |
| 5.2 Rischi e misure di sicurezza | 5060 |
| 5.2.1 L’architettura di sicurezza dei sistemi cantonali | 5060 |
| 5.2.1.1 Catalogo elettorale virtuale | 5060 |
| 5.2.1.2 Carte di legittimazione | 5061 |
| 5.2.1.3 Identificazione, autorizzazione e validazione | 5061 |
| 5.2.1.4 Criptaggio e decriptazione dei voti | 5061 |
| 5.2.1.5 Sistema di memorizzazione ridondante | 5062 |
| 5.2.1.6 Verifica del diritto di voto nel seggio elettorale | 5062 |
| 5.2.1.7 Verifica della plausibilità | 5063 |
| 5.2.1.8 Decriptazione dei voti | 5063 |
| 5.2.1.9 Sistema di determinazione dei risultati | 5063 |
| 5.2.1.10 Protezione dei dati | 5063 |
| 5.2.2 Valutazione dell’attuazione cantonale con riferimento ai rischi | 5064 |
| 5.2.2.1 Identificazione e autenticazione della persona avente diritto di voto | 5064 |
| 5.2.2.2 Autenticazione del server di voto | 5065 |
| 5.2.2.3 Comunicazione sicura | 5065 |
| 5.2.2.4 Sicurezza degli apparecchi di immissione | 5066 |
| 5.2.2.5 Controllo democratico del processo di spoglio | 5066 |
| 5.2.2.6 Tracciabilità e verificabilità | 5067 |
| 5.2.3 Confronto con i rischi del voto per corrispondenza | 5069 |
| 5.3 Economicità e fattibilità | 5074 |
| 5.3.1 Costi dei progetti pilota | 5074 |
| 5.3.2 Costi dell’introduzione del voto elettronico | 5077 |
| 5.3.3 Potenziale di risparmio | 5079 |
| 5.3.4 Due varianti di collaborazione tra i Cantoni | 5081 |
| 5.3.5 Armonizzazione dei cataloghi elettorali e identificatore delle persone | 5081 |
| 5.4 Considerazioni conclusive e ulteriore procedura | 5082 |
| 5.4.1 Realizzazione graduale | 5083 |
| 5.4.2 Necessità di adeguare le basi legali | 5084 |
| 5.4.3 Misure di accompagnamento di politica sociale | 5085 |
| 5.4.4 Organizzazione dei lavori successivi | 5086 |

| | |
|-------------------------------------|-------------|
| 6 Considerazione conclusiva | 5086 |
| Glossario tecnico | 5089 |
| Documentazione complementare | 5091 |

Rapporto

1 Situazione iniziale

Nel quadro del rapido sviluppo delle tecnologie dell'informazione e della comunicazione negli anni Novanta, la Svizzera ha mostrato un interesse crescente per le possibilità che le conquiste tecniche potevano rappresentare per la gestione dell'Amministrazione, la comunicazione tra cittadini e Stato e il processo democratico di formazione delle opinioni e delle decisioni.

In questo contesto, la Cancelleria federale, su incarico del Consiglio federale e del Parlamento e in collaborazione con i Cantoni di Ginevra, Neuchâtel e Zurigo, ha eseguito prove pilota e valutato la fattibilità del voto elettronico in Svizzera.

1.1 Che cos'è il voto elettronico?

La rapida diffusione di mezzi di comunicazione digitali consente nuove possibilità di interazione e informazione nella quotidianità professionale e privata. Le nuove tecnologie dell'informazione e della comunicazione non si fermano neppure alle porte della cultura democratica della Svizzera. In particolare, la rete Internet ha già modificato radicalmente la quotidianità politica. Sempre più informazioni politiche sono messe a disposizione e consultate on line. I partiti sono esposti alla concorrenza digitale proprio come i politici. Il processo di formazione delle opinioni nella società passa in misura sempre maggiore attraverso Internet. Di conseguenza, occorre domandarsi in che modo lo Stato debba garantire la partecipazione politica dei cittadini nella democrazia digitale.

Il voto elettronico per votazioni ed elezioni politiche al di fuori del seggio elettorale rappresenta una possibile risposta. Le prime applicazioni sono note: le votazioni in Parlamento sono svolte mediante computer e tabelloni elettronici e in molti Paesi sono già utilizzate macchine di voto elettroniche con schermo a sfioramento (touch screen)¹. Un'ulteriore possibilità consiste nel votare da postazioni pubbliche (chioschi) per mezzo di computer appositamente attrezzati e gestiti da autorità pubbliche.

L'impiego delle macchine di voto e del voto da chioschi pubblici tuttavia non riveste grande importanza in Svizzera visto che tutti possono votare per corrispondenza. Di conseguenza, queste possibilità non sono state sperimentate nell'ambito dei progetti pilota.

In Svizzera quando si parla di voto elettronico, si intende piuttosto il cosiddetto «remote electronic voting»², cioè il voto via Internet, SMS e altri canali elettronici di comunicazione dati.

¹ Cfr. n. 4.4

² Per designare questa forma di voto elettronico si utilizza l'espressione «voto elettronico a distanza» o nell'area linguistica anglofona «remote e-voting» oppure «remote voting by electronic means (RVEM)».

Infine fanno parte del voto elettronico anche la firma digitale di iniziative e referendum e le proposte di elezione nel Consiglio nazionale. Queste procedure non sono state sottoposte a test nel corso della fase pilota conclusa. Per la firma elettronica occorre eventualmente una firma digitale riconosciuta dallo Stato, dato che proprio in questo caso non è la segretezza del voto a essere indispensabile, ma l'identificazione del nome della persona che firma. Le firme elettroniche qualificate non sono ancora sufficientemente diffuse in Svizzera³.

1.2 Mandato del Parlamento

Nella Strategia del 18 febbraio 1998 per una società dell'informazione in Svizzera, il nostro Collegio sosteneva che si doveva esaminare in che misura sarebbe stato possibile utilizzare le tecnologie di informazione e comunicazione nel processo democratico di ricerca del consenso⁴. Due anni dopo, il Parlamento ha chiesto la realizzazione di uno studio sulla fattibilità, invitando il Consiglio federale a incoraggiare i preparativi per l'introduzione del voto elettronico in Svizzera⁵.

Nell'agosto 2000 abbiamo incaricato la Cancelleria federale di esaminare la fattibilità del voto elettronico quale voto al di fuori del seggio elettorale attraverso una rete (p. es. Internet) da qualsiasi apparecchio. In virtù di una decisione della Cancelleria federale del 30 giugno 2000 è stato istituito un gruppo di lavoro «progetto preliminare di voto elettronico» con rappresentanti della Confederazione e dei Cantoni.

Successivamente il gruppo di lavoro ha raccolto informazioni su progetti analoghi realizzati all'estero, ha esaminato le varianti tecniche necessarie per garantire la sicurezza, ha valutato i possibili rischi e le opportunità del voto elettronico, ha chiarito le possibilità di creare un catalogo elettorale virtuale e ha fatto le prime stime dei costi in caso di introduzione del voto elettronico. Il 9 gennaio 2002 abbiamo presentato al Parlamento il rapporto sul voto elettronico: le opportunità, i rischi e la fattibilità dell'esercizio dei diritti politici per via elettronica (FF 2002 567), in cui siamo giunti alla conclusione che per chiarire in modo definitivo la fattibilità si dovevano realizzare progetti pilota con i Cantoni interessati.

La Commissione delle istituzioni politiche del Consiglio nazionale, incaricata dell'esame preliminare, ha sostenuto tale proposta. Secondo la Commissione, tuttavia, la via verso il voto elettronico si deve intraprendere a piccole tappe per poter tenere conto delle particolarità del sistema politico svizzero (democrazia diretta e federalismo). La fiducia dei votanti nella democrazia semidiretta non deve essere incrinata. Per quanto riguarda i rischi del voto elettronico, secondo la Commissione si devono tollerare gli stessi rischi che comporta il voto per corrispondenza. Il Consiglio

³ Con l'entrata in vigore, il 1° gennaio 2005, della legge sulla firma elettronica, (FiEle; RS 943.03) è creata la base giuridica per transazioni vincolanti dirette. Swisscom Solutions del Gruppo Swisscom è la prima società in Svizzera che ha ricevuto nel dicembre 2005 la certificazione quale fornitore di servizi per firme elettroniche certificate.

⁴ Strategia del 18 febbraio 1998 per una società dell'informazione in Svizzera, pag. 3. Con il 7° rapporto del gruppo di coordinamento Società dell'informazione, abbiamo ha riveduto la nostra strategia il 18 gennaio 2006. In tale occasione abbiamo riaffermato che le tecnologie dell'informazione e della comunicazione possono migliorare le possibilità di comunicazione e di partecipazione di tutti i cittadini (cfr. www.infosociety.ch).

⁵ Per i diversi interventi, cfr. il rapporto del 9 gennaio 2002 sul voto elettronico: le opportunità, i rischi e la fattibilità dell'esercizio dei diritti politici per via elettronica, FF 2002 567, qui pag. 571 seg.

nazionale ha preso conoscenza del rapporto il 19 marzo 2002 e il Consiglio degli Stati, il 5 giugno 2002⁶.

2 Condizioni per lo svolgimento di prove pilota

Qui di seguito sono presentate le condizioni che devono essere soddisfatte per lo svolgimento di prove pilota in materia di voto elettronico.

2.1 Basi legali per lo svolgimento di prove pilota

Il 21 giugno 2002, nell'ambito di una revisione parziale della legge federale del 17 dicembre 1976 sui diritti politici (LDP, RS 161.1), il Parlamento ha creato le basi legali per lo svolgimento di prove pilota vincolanti di voto elettronico⁷. D'intesa con i Cantoni e i Comuni interessati, il Consiglio federale può autorizzare prove pilota limitate sotto il profilo territoriale, temporale e materiale. In particolare il controllo della legittimazione al voto, il segreto del voto e lo spoglio di tutti i voti devono essere garantiti e gli abusi esclusi. Contemporaneamente, il Parlamento ha chiesto che la sperimentazione del voto elettronico fosse sorretta da una consulenza scientifica, in particolare che venissero rilevati dati concernenti sesso, età e formazione.

In esecuzione del nuovo articolo 8a LDP, il 20 settembre 2002 sono state definite mediante modifica dell'ordinanza del 24 maggio 1978 sui diritti politici (ODP, RS 161.11) le esigenze che devono essere soddisfatte affinché il nostro Collegio possa autorizzare lo svolgimento di prove pilota del voto elettronico (art. 27a–27g ODP, RU 2002 3200). Le istruzioni per l'applicazione sono state comunicate dal Consiglio federale ai Cantoni con Circolare del 20 settembre 2002 (FF 2002 5891).

2.2 Convenzioni con i Cantoni pilota

Abbiamo convenuto con i Cantoni di Ginevra, Neuchâtel e Zurigo, in una dichiarazione di intenti, l'istituzione di progetti pilota volti a preparare, in tutti e tre i Cantoni, prove giuridicamente vincolanti in occasione di votazioni popolari federali. L'esecuzione dei progetti è stata regolata nei contratti stipulati tra la Cancelleria federale e i tre Cantoni. Accanto alle misure di sicurezza da osservare, deve essere garantito che:

- voti espressi per via elettronica non possano essere intercettati, modificati o deviati in modo sistematico;
- terzi non possano venire a conoscenza del contenuto di voti espressi per via elettronica;

⁶ Boll. Uff. 2002 N 331 segg. e 1139; Boll. Uff. 2002 S 333 segg. e 553.

⁷ Art. 5 cpv. 3 secondo periodo, art. 8a, art. 12 cpv. 3, art. 38 cpv. 5 e art. 49 cpv. 3 LDP come pure art. 1 cpv. 1 secondo periodo della legge federale del 19 dicembre 1975 sui diritti politici degli Svizzeri all'estero (LDPSE, RS 161.5). RU 2002 3193.

- possano partecipare allo scrutinio soltanto gli aventi diritto di voto;
- ciascun avente diritto di voto disponga di un solo voto.

Secondo esplicita disposizione contrattuale, i progetti pilota non pregiudicano in alcun modo una futura soluzione a livello federale. Dall'autorizzazione di eseguire una prova pilota, i Cantoni non possono desumere nessuna autorizzazione generale per un'eventuale introduzione del voto elettronico sul loro territorio. La Confederazione partecipa ai costi supplementari provocati dalle prove pilota rispetto alle votazioni tradizionali nella misura dell'80 per cento al massimo. È stato anche convenuto per contratto che tutti i Cantoni interessati possono disporre gratuitamente dei risultati dei progetti pilota.

2.3 Procedura di autorizzazione di prove pilota da parte del Consiglio federale

L'autorizzazione di progetti pilota in occasione di votazioni federali spetta al Consiglio federale (art. 27c periodo introduttivo ODP), che, in virtù della legge, accerta vincolativamente il risultato della votazione (art. 15 cpv. 1 LDP). Per minimizzare i rischi, il Consiglio federale può autorizzare la sperimentazione del voto elettronico limitandola sotto il profilo territoriale, temporale e materiale. Stabilisce tra l'altro, per quali Comuni i risultati dell'elezione o della votazione ottenuti nell'ambito della prova pilota hanno effetto giuridicamente vincolante sull'esito a livello di Confederazione (art. 27c cpv. c ODP) e per quali votazioni federali è ammesso il voto elettronico (art. 27c cpv. a ODP). Con la modifica del 20 settembre 2002 dell'ordinanza, abbiamo subordinato l'autorizzazione a severe condizioni che devono essere adempiute cumulativamente, sempreché l'ordinanza non disponga espressamente altrimenti⁸.

I progetti pilota dei Cantoni di Ginevra, Neuchâtel e Zurigo sono stati realizzati in stretta collaborazione con la Cancelleria federale. La Cancelleria federale e i gruppi di monitoraggio dei Cantoni erano costantemente informati dello stato tecnico e degli eventuali adeguamenti previsti.

Ogni impiego del voto elettronico previsto nell'ambito di votazioni federali durante la fase pilota era subordinato all'autorizzazione del Consiglio federale. Le necessarie domande di autorizzazione dovevano contenere, tra l'altro, documentazioni tecniche dettagliate.

Su incarico della Cancelleria federale, ditte esterne hanno controllato la sicurezza e la protezione contro attacchi di hacker dei tre sistemi pilota, prima che venissero impiegati la prima volta. La verifica della plausibilità (cfr. n. 5.2.1.7), la domenica

⁸ Per la protezione contro i rischi, un sistema di voto elettronico deve essere conforme allo stato più recente della tecnica ed essere controllato regolarmente da un ente esterno indipendente. All'articolo 27/ «Stato della tecnica» l'ODP stabilisce quanto segue:
 cpv. 1: «prima di ogni votazione o elezione, i componenti tecnici utilizzati dalle autorità competenti, i software, l'organizzazione e lo svolgimento della procedura devono essere valutati secondo lo stato più recente della tecnica»;
 cpv. 2: «un ente esterno indipendente riconosciuto dalla Cancelleria federale deve confermare che i requisiti in materia di sicurezza sono soddisfatti e che il sistema di voto elettronico impiegato funziona. Questa esigenza si applica anche a ogni modifica del sistema».

della votazione, si è sempre svolta alla presenza di rappresentanti della Cancelleria federale.

Per quanto riguarda la documentazione tecnica per un sistema di voto elettronico e le perizie in materia di sicurezza, si tratta di documenti confidenziali dei Cantoni che vengono sottoposti per visione al nostro Collegio. Questi documenti non sono pubblici. I Cantoni in cui il principio della trasparenza è già applicato possono subordinare la visione di questi documenti o il codice di programma a determinate condizioni, oppure negarli nella misura in cui si tratti di informazioni sensibili relative alla sicurezza o di segreti di fabbrica. Tale prassi è stata confermata dal Tribunale federale⁹.

2.4 Armonizzazione dei cataloghi elettorali e identificatore delle persone

Una condizione molto importante per il voto elettronico è l'armonizzazione dei cataloghi elettorali gestiti nella maggior parte dei casi nei Comuni¹⁰. Al momento in cui sono stati intrapresi i lavori pilota non esistevano a livello federale convenzioni legali per l'identificazione delle persone in questi cataloghi né per le designazioni dei campi, le caratteristiche e le grafie. Per sviluppare le loro applicazioni, i Cantoni pilota hanno però potuto avvalersi sia di disposizioni cantonali sia di uno standard dell'associazione eCH¹¹. Per l'identificazione delle persone sono stati utilizzati identificatori cantonali o comunali. Lo scambio di dati a livello superiore tra i cataloghi elettorali non era possibile a causa della mancanza di un'identificazione numerica unitaria.

Il Cantone di Ginevra disponeva, già all'inizio del progetto, di un registro cantonale uniforme delle persone, dal quale, il giorno prestabilito, veniva creato un catalogo elettorale. Nel Cantone di Neuchâtel l'unificazione dei registri gestiti da ogni singolo Comune è stata portata a termine poco prima che il progetto venisse lanciato. Nel Cantone di Zurigo infine si è dovuto prima sviluppare un quadro (view) cantonale dei registri comunali nell'ambito del progetto.

Per garantire il segreto del voto, dopo la generazione delle carte di legittimazione nei tre Cantoni pilota tutti i dati personali (nome, indirizzo, data di nascita ecc.) sono stati resi anonimi. Mediante il numero della carta di legittimazione si è potuto controllare nel catalogo elettorale se qualcuno aveva già esercitato il diritto di voto e impedire così che votasse due volte. Né prima né durante o dopo la votazione con il voto elettronico vi sono altre possibilità di risalire alle persone che hanno votato.

⁹ Sentenza del Tribunale federale 1P.29/2006 del 23 marzo 2006, non pubblicata.

¹⁰ Per lo stato delle basi legali cantonali in materia di gestione dei cataloghi elettorali, cfr. la documentazione complementare 3.

¹¹ eCH-Standard «0027:Meldeprozesse», in vigore dal 29.10.2004, www.unisg.ch/org/idt/echweb.nsf/0/D38E4752D42D358AC1256F3C002F6B0A?OpenDocument&lang=de.

2.5 Esigenze relative al diritto in materia di protezione dei dati

Secondo l'Incaricato federale della protezione dei dati (IFPD), il voto elettronico è un'applicazione molto complessa, in cui l'anonimato dei votanti richiesto dal segreto del voto, da una parte, e l'esigenza di una certa verificabilità del risultato della votazione dall'altra sono in conflitto fra loro. L'IFPD ha valutato criticamente il voto elettronico per la prima volta nel rapporto di attività 2002: noti esperti informatici mettono in dubbio la tracciabilità di processi informatici nell'ambito del voto elettronico. L'IFPD richiama l'attenzione sulle cosiddette firme cieche, che pur consentono di superare o di attenuare in qualche modo la contraddizione tra anonimato e tracciabilità: la complessità non è, tuttavia, ancora risolta integralmente dal punto di vista tecnico. Prima di introdurre il voto elettronico, si deve verificare la sua fattibilità proprio in questo ambito¹².

Scopo della legge federale del 19 giugno 1992 sulla protezione dei dati (LPD, RS 235.1) è, conformemente agli articoli 1 e 2, proteggere la personalità e i diritti fondamentali delle persone i cui dati sono oggetto di trattamento da parte di organi federali o terzi privati. Secondo l'articolo 4, i dati personali possono essere raccolti e trattati soltanto in modo lecito e per lo scopo previsto da una legge.

Ciò riguarda in primo luogo i dati necessari per elaborare i cataloghi elettorali dai registri degli abitanti dei Comuni e dei Cantoni. In secondo luogo, tuttavia, sono rilevanti dal punto di vista della protezione dei dati anche i dati necessari per il controllo del diritto di voto al momento della sua espressione. Nel primo caso per il voto elettronico ci si può avvalere della vasta esperienza acquisita nell'ambito delle procedure di voto esistenti. Soltanto nei casi in cui i cataloghi elettorali sono costituiti esplicitamente per il voto elettronico, ad esempio a livello cantonale, è necessario riconsiderare il loro trattamento dal punto di vista del diritto in materia di protezione dei dati.

3 Criteri di valutazione

Nel presente capitolo sono esposti i criteri in base ai quali i progetti pilota sono stati valutati. I progetti pilota sono descritti nel numero 4 e valutati nel numero 5 in base ai criteri qui presentati.

3.1 Utilità e ripercussioni sulla democrazia diretta

L'utilità del voto elettronico è ravvisata, di regola, nella semplificazione dell'operazione di voto. In una società sempre più mobile, il voto elettronico, come già quello per corrispondenza, può facilitare notevolmente la partecipazione a votazioni ed elezioni. Molti giovani, ma anche i cittadini di una certa età, potrebbero optare per questa moderna variante di voto, più consona alle abitudini di vita della società dell'informazione. Per molti Svizzeri all'estero, il voto elettronico eliminerebbe l'inconveniente dei lunghi tempi di consegna della posta internazionale. Le persone

¹² 9° rapporto dell'Incaricato federale della protezione dei dati 2001/2002, Berna 2002, pag. 14 seg. (documento completo solo in tedesco e in francese); www.edsb.ch.

non vedenti e ipovedenti, infine, potrebbero per la prima volta partecipare¹³ a votazioni ed elezioni senza ricorrere all'aiuto di terzi, serbando il segreto di voto. Di conseguenza, il voto elettronico potrebbe contribuire all'aumento della partecipazione elettorale.

Accanto all'utilità generale di un possibile aumento della partecipazione vi sono però anche aspetti di utilità parziale. Se il voto elettronico incoraggiasse gruppi specifici della popolazione (p. es. i giovani, gli anziani, gli uomini, le donne, le persone orientate a valori di tipo postmaterialista o le persone di stampo tradizionale ecc.) a partecipare a votazioni ed elezioni in maniera nettamente più massiccia rispetto alla media attuale oppure li inducesse addirittura a votare regolarmente, alcuni partiti e gruppi di interesse potrebbero beneficiarne più di altri.

La consulenza scientifica relativa alle prove pilota doveva inoltre permettere di appurare se il voto elettronico trova consensi e corrisponde a un'esigenza degli elettori.

Nell'ambito dell'ultima revisione della legge federale sui diritti politici, il Parlamento ha pertanto completato l'articolo 8a con un corrispondente capoverso 3 nel quale si esige in particolare che siano rilevati dati concernenti sesso, età e formazione delle persone che partecipano alle prove pilota.

La Cancelleria federale ha dovuto stabilire le condizioni quadro (costi, obiettivi) dei rilevamenti scientifici collaterali concernenti il profilo sociodemografico dei partecipanti alle prove pilota del voto elettronico. Inoltre ha provveduto a far verificare l'efficacia delle prove pilota, segnatamente per quanto concerne l'evoluzione della partecipazione e l'incidenza sulle abitudini di voto (art. 27o-27p ODP).

3.2 Protezione contro i rischi e gli abusi

Il voto elettronico deve soddisfare esigenze molto elevate in materia di sicurezza. La scienza si è occupata intensamente dei rischi del voto elettronico. Figurano al primo posto i rischi di manipolazione tecnica e una generale messa in pericolo della democrazia.

Si potrebbe manipolare l'apparecchio impiegato per la votazione in modo tale che le caratteristiche di voto e le informazioni che consentono di identificare il votante possano essere memorizzate e spiate¹⁴. Questo rischio appare elevato perché gli apparecchi utilizzati per il voto si trovano fuori dall'ambito di controllo delle autorità di votazione ed elezione e si presume che i votanti non abbiano necessariamente

¹³ È quanto risulta da un'inchiesta svolta nel febbraio 2002 presso la fondazione «Accesso per tutti». Per poter esprimere il voto occorre tuttavia un apparecchio dotato di tastiera Braille e sintesi vocale. La persona ipovedente potrebbe leggere mediante uno scanner anche i codici che figurano sulla carta di legittimazione.

¹⁴ FF 2002 590; Alvarez/Hall 2004, pag. 83; Jefferson et al. 2004a, pag. 62; Jefferson et al. 2004b, pag. 12 segg.; Mitchison 2003, pag. 259; Oppliger 2002b, pag. 12 e 18 seg.; Oppliger 2002a, pag. 185; Comité Sécurité (28.1.2002), pag. 7 seg.; Rubin 2002, pag. 40 segg.; Schryen 2004, pag. 124 seg. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.

conoscenze sufficienti per riconoscere software o attacchi maligni¹⁵. Un ulteriore rischio è la vulnerabilità alle simulazioni (cosiddetto «spoofing»). Gli aventi diritto di voto potrebbero giungere su pagine internet contraffatte e immettervi il voto e i dati di accesso. Grazie alle informazioni così acquisite, persone non autorizzate potrebbero sostituirsi al votante (attacco man-in-the-middle)¹⁶ per immettere le loro preferenze politiche nel server ufficiale di voto. Un attacco analogo potrebbe consistere nell'intromettersi, senza essere identificati, nella comunicazione dati tra il server ufficiale di voto e il votante per manomettere il voto. Nelle reti aziendali gli amministratori del sistema potrebbero cercare di osservare i collaboratori mentre votano o cercare di contraffare il voto¹⁷. Infine si potrebbero utilizzare i dati della memoria intermedia di un apparecchio di immissione per conoscere il voto effettivamente espresso da una persona¹⁸.

In una perizia del 2004 sul sistema di voto elettronico SERVE degli USA si giunge alla conclusione che, così come è concepita, la rete Internet non è idonea alla comunicazione sicura e protetta¹⁹. L'intrusione anche in reti considerate altamente sicure (di ditte high tech, governi ecc.) ha mostrato che gli esperti di computer trovano sempre nuovi mezzi per superare le barriere di sicurezza di un sistema. Ciò potrebbe interessare non solo i partiti politici, ma anche i terroristi o gli Stati terzi²⁰. Tra le persone potenzialmente pericolose figurano però anche gli «insider», come gli amministratori del sistema o i collaboratori delle ditte di produzione, che si procurano un accesso non autorizzato ai dati²¹, sia per interesse personale sia perché costretti²². Anche sulla verificabilità dei processi nell'ambito del voto elettronico si nutrono forti dubbi. Solo gli addetti ai lavori, ad esempio gli informatici²³, sono in grado di capire come funzionano il conteggio e gli eventuali riconteggi dei voti. Ciò può incrinare la fiducia dell'elettorato²⁴. Abbiamo già presentato un elenco completo di

- 15 Cfr. Burmester/Magkos 2003, pag. 67; Cranor 2003, pag. 27; Independent Commission on Alternative Voting Methods (U.K.) 2002, pag. 91 seg.; Jefferson et al. 2004a, pag. 62 seg.; Jones 2003, pag. 14; Comité Sécurité (28.1.2002), pag. 8; Rubin 2002, pag. 40. Per il fattore «uomo» nel settore della sicurezza digitale cfr. Schneier 2004, pag. 249 segg. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 16 Alvarez/Hall 2004, pag. 84; Burmester/Magkos 2003, pag. 67; Independent Commission on Alternative Voting Methods (U.K.) 2002, pag. 92; Jefferson et al. 2004a, pag. 63; Jefferson et al. 2004b, pag. 16 segg. Mitchison 2003, pag. 259; Oppliger 2002a, pag. 185; Comité Sécurité (28.1.2002), pag. 7 seg.; Rubin 2002, pag. 41 e 43 seg.; Schryen 2004, pag. 127. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 17 Jefferson et al. 2004b, pag. 13 seg.; Oppliger 2002b, pag. 12. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 18 Cfr. anche Burmester/Magkos 2003, pag. 73; Peralta 2003, pag. 156 e 158. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 19 Jefferson et al. 2004a, pag. 60; Jefferson et al. 2004b, pag. 21 e 32. Come pure Kley/Feller 2003, pag. 98. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 20 Jefferson et al. 2004b, pag. 11; Pratchett et al. 2005, pag. 171. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 21 Cfr. Mitchison 2003, pag. 260 seg.; Pratchett et al. 2005, pag. 172; Rubin 2002, pag. 42. Cfr. anche Schneier 2004, pag. 44 seg. e 259. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 22 Comité Sécurité (28.01.2002), pag. 9. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 23 FF 2002 582; Flückiger 2003, pag. 146 segg.; Kley/Rütsche 2002, pag. 271; Steinmann 2003, pag. 500; Warynski 2003, pag. 232. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.
- 24 Kley/Feller 2003, pag. 98 seg.; Steinmann 2003, pag. 500. Per i riferimenti bibliografici completi, cfr. la documentazione complementare 1.

questi rischi e pericoli nel nostro rapporto del 9 gennaio 2002²⁵ sul voto elettronico. Anche nei dibattiti parlamentari sul rapporto e sulla base legale per prove pilota del voto elettronico si sono levate voci critiche sulle questioni della sicurezza, dell'impedimento di abusi e della tutela del segreto nell'ambito del voto elettronico²⁶.

In occasione di un convegno organizzato nell'ottobre 2002 dall'Associazione svizzera d'informatica giuridica le persone che contestano il voto elettronico hanno manifestato le loro preoccupazioni, in particolare per la trasmissione segreta dei voti espressi per via elettronica²⁷.

Il voto elettronico per la Svizzera deve soddisfare le più elevate esigenze di sicurezza. Contemporaneamente deve poter essere utilizzato anche dagli aventi diritto di voto che non hanno conoscenze specialistiche. In questo contesto deve essere assicurato il massimo grado di sicurezza a un prezzo abbordabile e senza ridurre eccessivamente l'usabilità. Nell'ambito delle prove pilota, i possibili rischi del voto elettronico e le relative misure di sicurezza sono stati pertanto valutati e confrontati con i rischi e le misure adottate per le modalità di voto tradizionali, in particolare quello per corrispondenza.

Riassumendo si possono classificare i rischi tecnici da analizzare nell'ambito delle prove pilota di voto elettronico nelle seguenti categorie di problemi:

- identificazione e autenticazione dell'elettore
- autenticazione del server di voto
- comunicazione sicura
- sicurezza degli apparecchi di immissione
- controllo democratico del processo di spoglio
- tracciabilità e verificabilità

3.3 Economicità e fattibilità politica

Nel nostro rapporto del 9 gennaio 2002 sul voto elettronico, abbiamo stimato a 400–620 milioni di franchi i costi per l'introduzione capillare del voto elettronico in Svizzera e per un esercizio di dieci anni²⁸. Si pensava di poter realizzare l'introduzione capillare in pochi anni.

Nei dibattiti parlamentari è stato sostenuto da più parti che non era ragionevole realizzare un progetto così costoso; la situazione finanziaria delle amministrazioni pubbliche in Svizzera è peggiorata drasticamente negli ultimi due decenni; in considerazione dell'elevato debito pubblico, i progetti di tali dimensioni devono essere sottoposti a un esame approfondito.

²⁵ FF **2002** 567, qui 575 seg.

²⁶ Boll. Uff. **2002** N 333

²⁷ Cfr. Murali Müller Hanna e Koller Thomas (Editori), E-Voting, Tagung 2002 für Informatikrecht, Berna 2002.

²⁸ FF **2002** 608 seg.

Date queste premesse, era necessario rivedere la valutazione sommaria fatta nel rapporto del 9 gennaio 2002 sul voto elettronico. In particolare al momento di realizzare i progetti pilota, si dovevano rilevare le spese di personale e di materiale sostenute per lo sviluppo e l'implementazione dei sistemi cantonali e per lo svolgimento di votazioni con il voto elettronico e valutarle in vista di un'eventuale introduzione generale del voto elettronico in Svizzera.

Contemporaneamente si doveva chiarire, nell'ambito delle prove pilota, la capacità delle amministrazioni di soddisfare ai tre livelli dello Stato le condizioni necessarie per la realizzazione del voto elettronico e la volontà politica per questo impegno non irrilevante e per la necessaria collaborazione.

4 Prove pilota negli anni 2004 e 2005

4.1 Il progetto pilota del Cantone di Ginevra

4.1.1 Condizioni quadro

In una dichiarazione di intenti del 25 aprile 2001 abbiamo palesato la nostra disponibilità a rilasciare al Governo del Cantone di Ginevra, su richiesta, l'autorizzazione per lo svolgimento di una prova pilota del voto elettronico in occasione di una votazione federale non appena i mezzi tecnici avessero consentito di garantire integralmente i principi in materia di voto ancorati nella Costituzione e nella legge²⁹.

Il concreto svolgimento del progetto pilota di Ginevra è stato regolato nel contratto stipulato il 25 aprile 2001 tra la Cancelleria federale e il Cantone di Ginevra. Obiettivo del progetto pilota era di fornire la prova che, impiegando una combinazione univoca di codice di accesso e di password e adottando altre misure tecniche e organizzative, si poteva assicurare un voto elettronico sicuro in occasione di votazioni federali.

4.1.2 Basi legali e condizioni cantonali

Quando ha lanciato il suo progetto pilota, il Cantone di Ginevra disponeva già di una base legale per l'autorizzazione di prove pilota del voto elettronico: la legge cantonale del 1982 sui diritti politici conteneva un articolo 188 che consentiva di eseguire prove a livello cantonale e comunale al fine di adeguare l'esercizio dei diritti politici e lo spoglio dei voti all'evoluzione tecnica³⁰. Ne fa parte, logicamente, anche il voto elettronico. Ogni impiego del voto elettronico deve essere autorizzato dal Consiglio di Stato³¹.

La legislazione del Cantone di Ginevra consente ai cittadini di assistere allo spoglio dei voti nel seggio elettorale. Per il voto per corrispondenza, il controllo pubblico è stato delegato ai partiti, che formano con i loro membri un gruppo di «controllori». Questo procedimento è stato esteso alle prove pilota del voto elettronico.

²⁹ Cfr. n. 2.2

³⁰ Art. 188 Loi sur l'exercice des droits politiques du 15 octobre 1982 (LEDP), Recueil systématique genevois A 5 05.

³¹ Cfr. ad es. www.geneve.ch/evoting/doc/ace_autorisation.pdf.

4.1.3

Soluzione e realizzazione

Il sistema di voto elettronico sviluppato dal Cantone di Ginevra è di proprietà del Cantone stesso. È stato sviluppato su incarico della Cancelleria dello Stato dal servizio di informatica del Cantone (Centre des technologies de l'information de l'Etat [CTI]) in collaborazione con ditte private con sede a Ginevra: Hewlett Packard Svizzera (hardware e software), Wisekey (tecnologia di criptaggio) e blueinfinity (sicurezza).

Il concetto chiave che ha caratterizzato lo sviluppo della soluzione di voto elettronico di Ginevra è stato quello dell'usabilità. Per reggere il confronto con il voto per corrispondenza, quello elettronico deve essere, per quanto possibile, altrettanto semplice. Il lavoro è consistito nel trasporre su Internet la procedura del voto per corrispondenza. La carta di legittimazione esistente, riprodotta per ogni scrutinio, è stata modificata leggermente e adattata al voto elettronico.

Dei tre Cantoni pilota, Ginevra era il solo a disporre di un catalogo informatizzato degli elettori al momento del lancio del progetto di voto elettronico. Questo catalogo non esiste in maniera duratura, ma viene creato, prima di ogni scrutinio, dal registro degli abitanti gestito dall'Ufficio cantonale della popolazione, da una parte, e dal registro degli Svizzeri all'estero, gestito dal Servizio delle votazioni ed elezioni, dall'altra. La situazione di Ginevra è simile a quella di molti Cantoni svizzeri, ai quali potrebbe dunque servire da base.

Il catalogo elettorale caricato sui server di voto è reso anonimo. Gli elettori sono registrati mediante un numero personale di sedici cifre, che permette di criptare l'anno di nascita, il sesso e il Comune in cui esercitano il diritto di voto. Questo numero personale è riprodotto sulla carta di legittimazione assieme a un codice segreto di sei cifre nascosto sotto un'area da grattare e al fingerprint del certificato del server. Quest'ultimo permette agli elettori di assicurarsi di essere veramente in contatto con il sito ufficiale di voto.

Il voto via Internet si svolge in 4 tappe:

1. per essere ammesso sul server di voto, l'elettore deve immettere il suo numero personale di sedici cifre. La probabilità di indovinare la combinazione giusta è di uno su cinque miliardi. Superato questo controllo, viene stabilito il collegamento con il server protetto e una scheda di voto elettronica è inviata al PC dell'elettore;
2. l'elettore vota;
3. il sistema propone all'elettore una ricapitolazione delle scelte. L'elettore deve identificarsi con la data di nascita e il Comune di appartenenza (da scegliere da un menu con 50 Comuni) e il codice segreto che figura sulla carta di legittimazione, sotto una zona da grattare. Questo codice cambia per ogni scrutinio;
4. il sistema conferma di aver registrato il voto e indica la data e l'ora della registrazione.

Dato che il catalogo elettorale è lo stesso per il voto per corrispondenza e per quello elettronico, il voto via Internet annulla la possibilità di registrare un voto per corrispondenza per la stessa persona e, considerato che per confermare il voto espresso via Internet si deve scoprire il codice segreto, è evidente che votando on line si

lascia una «traccia». Di conseguenza, l'elettore che presenta al seggio elettorale una carta di legittimazione con codice segreto scoperto non può votare senza che si sia prima verificato che non lo abbia già fatto.

Prima dell'apertura dello scrutinio, l'urna elettronica è chiusa con due chiavi digitali, la cui parola d'ordine è scelta dai controllori. Un controllo vicendevole fra i partiti e dei partiti sull'amministrazione viene esercitato al momento della chiusura e dell'apertura dell'urna. Durante lo scrutinio, l'accesso fisico al luogo in cui si trova l'urna elettronica è severamente controllato.

Inoltre, i controllori immettono voti in un'urna di prova, il cui spoglio deve dare il risultato atteso in termini di numero di voti. In questo modo è possibile verificare che l'applicazione non produca distorsioni dei risultati.

Lo spoglio dei voti elettronici ha luogo nell'edificio della Polizia cantonale, alla presenza dei controllori dei partiti politici. Un personal computer è collegato con l'urna elettronica attraverso un cavo di dati separato. Solo i controllori possono decifrare i voti immettendo le due parole d'ordine create quando hanno avviato la procedura di voto. Dopo la chiusura delle urne, i voti elettronici, quelli espressi per corrispondenza e quelli depositati nelle urne sono sommati.

Un apposito sistema di sorveglianza controlla costantemente il sistema e i suoi componenti per quanto riguarda il corretto funzionamento, eventuali processi di errore oppure attacchi di hacker. Se subentrano irregolarità durante la procedura di voto, i responsabili del sistema sono allarmati automaticamente e operano secondo un programma di misure predefinito. Se non è possibile escludere ogni pericolo per l'urna elettronica, uno stato maggiore di crisi creato per ogni votazione può addirittura disconnettere il collegamento fisico del sistema dall'accesso internet. Al termine di ogni votazione, il numero di diritti di voto contrassegnati nel catalogo elettorale deve corrispondere al numero di voti memorizzati in forma cifrata nell'urna elettronica (tolleranza zero). Se non vi è corrispondenza totale, si deve analizzare il funzionamento del sistema per tutta la durata della votazione secondo i processi di sistema registrati su protocollo.

Le principali misure di sicurezza sono:

- su Internet la scheda di voto è criptata con l'aggiunta casuale di caratteri alfanumerici al contenuto; la persona che riuscisse a impossessarsene (evenienza assai improbabile) vedrebbe solo una serie di caratteri senza significato;
- la scheda rispedita all'elettore affinché possa confermare la sua scelta e identificarsi è combinata con un'immagine che la rende illeggibile agli hacker. L'immagine, diversa per ogni votante, consente all'elettore di verificare che è collegato con il sito ufficiale di voto;
- il sito di voto è certificato. Gli elettori possono vedere i certificati di autenticazione e hanno così una seconda possibilità di verificare con chi sono in contatto;
- l'identità degli elettori e le schede di voto sono conservate in due archivi distinti e separati;
- prima dell'apertura dell'urna di voto elettronico, il contenuto è modificato mediante algoritmo per cambiare l'ordine in cui le schede saranno decryptate e contate. In questo modo si impedisce la ricostruzione del voto di un deter-

minato elettore mediante il confronto dell'ordine di arrivo di una scheda di voto con l'ordine in cui un nome è notificato nell'archivio degli elettori che hanno votato;

- tutti gli elementi del sistema sono stati configurati in modo da rispondere solo a comandi conformi alla normale procedura di voto;
- il server è connesso alla rete solo il giorno dell'apertura dello scrutinio e disattivato alla chiusura dello stesso;
- tutta l'apparecchiatura è ridondante;
- tutti i dati sono memorizzati in doppio;
- i server si trovano in un locale protetto;
- l'accesso al server è riservato a un numero limitato di persone autorizzate dopo verifica;
- l'operatore non può accedere al server da solo: deve essere sempre accompagnato.

4.1.4 Prove pilota e lavori collaterali

Con il sistema di Ginevra sono state eseguite quattro prove interne all'amministrazione prima della primavera 2002. L'obiettivo era di sperimentare l'applicazione dei requisiti di sicurezza, la facilità d'uso del sistema e le misure collaterali adottate sul piano organizzativo. I risultati di queste prove interne hanno permesso di perfezionare sistematicamente il sistema e di eliminare errori nel programma di decriptazione.

Un'ulteriore prova pilota svolta nelle scuole, nel giugno 2002, ha dimostrato che il sistema di Ginevra può essere impiegato in modo sicuro nella rete pubblica di Internet.

Nell'anno 2001, il Cantone di Ginevra aveva affidato il suo sistema a un organo di controllo (Comitato di sicurezza) perché verificasse le misure di sicurezza; nel giugno 2002, la Cancelleria federale ha incaricato la società zurighese at Rete di provare la resistenza (vulnerabilità) del sistema a attacchi e manipolazioni. I funzionari cantonali con mansioni importanti sono stati inoltre interrogati sui loro obblighi di vigilanza. Il Cantone di Ginevra ha affidato alla ditta Hacknet l'incarico di eseguire procedure di test analoghe. Durante queste verifiche sono venuti alla luce diversi piccoli difetti che il Cantone di Ginevra ha potuto eliminare proprio prima della votazione comunale di Anières, nel gennaio 2003. I consulenti esterni hanno definito il sistema molto sicuro contro attacchi e abusi. Nessuno degli attacchi simulati è riuscito, nessun voto è stato intercettato, cancellato o manipolato durante i controlli.

In attesa della prima prova pilota in occasione di una votazione federale, il Cantone di Ginevra ha sperimentato il suo sistema nell'ambito di quattro votazioni comunali separate (a Anières, il 19 gennaio 2003, con 1162 aventi diritto di voto; a Cologny, il 30 novembre 2003, con 2521 aventi diritto di voto; a Carouge, il 18 aprile 2004, con 9049 aventi diritto di voto e a Meyrin, il 13 giugno 2004, con 9180 aventi diritto di voto). Questa serie di test è stata svolta con successo ed è continuata, in modo impeccabile e senza contestazioni, nell'ambito delle votazioni federali del 26 settembre 2004 (20 000 aventi diritto di voto) e del 28 novembre 2004 (40 000 aventi diritto di voto). Fino all'ultima prova, svolta contemporaneamente in 14 Comuni del

Cantone di Ginevra, il 17 aprile 2005, nell'ambito della votazione popolare cantonale, il numero di partecipanti è salito gradualmente a 88 000 unità. Mentre nelle prime prove svolte a Anières e Cologny oltre un terzo dei voti era stato espresso per via elettronica, nelle prove successive la quota dei voti elettronici si è stabilizzata tra il 22 e il 25 per cento³². Da un'inchiesta on line risulta che il 90 per cento circa degli elettori che aveva votato elettronicamente in una delle prime prove pilota è rimasto fedele al voto elettronico anche nelle successive.

Le prove pilota di Ginevra in occasione di votazioni federali si sono svolte con successo e senza difficoltà, suscitando grande risonanza nazionale e internazionale nei media e nel pubblico.

Il sistema di Ginevra è stato utilizzato otto volte con successo nell'ambito di votazioni a livello comunale, cantonale e federale. La prova pilota di Meyrin comprendeva una votazione su un'iniziativa con controprogetto e domanda risolutiva. In occasione del primo test nell'ambito di una votazione federale del 26 settembre 2004 si è potuto votare contemporaneamente a tutti e tre i livelli. Il sistema di Ginevra è in grado di gestire anche più votazioni contemporanee. Ciò è stato provato nell'ottobre 2004 a Vandoeuvres in occasione della votazione comunale durante la quale è stato svolto un sondaggio su incarico del Consiglio d'Europa. Nell'ambito del sondaggio per il Consiglio d'Europa sono stati registrati 16 000 voti in 10 giorni. Ciò corrisponde a due terzi del volume di voti previsto nel caso di un impiego capillare del sistema di Ginevra in occasione di una votazione popolare federale o cantonale nel Cantone di Ginevra.

4.1.4.1 Lavori collaterali

Sin dall'inizio, il progetto pilota del Cantone di Ginevra è stato seguito sistematicamente da un gruppo di monitoraggio composto di rappresentanti della Confederazione e dei Cantoni interessati e presieduto dalla Cancelleria federale. Il gruppo di monitoraggio aveva l'incarico di verificare le disposizioni organizzative e tecniche che il Cantone di Ginevra doveva osservare. Nell'ambito delle prime prove pilota nei Comuni di Anières, Cologny, Carouge e Meyrin, membri di questo gruppo di monitoraggio erano presenti in veste di osservatori, in particolare al momento del criptaggio dell'urna elettronica e dello spoglio dei voti espressi per via elettronica, la domenica della votazione.

Nell'ottobre 2004, la Società svizzera delle scienze amministrative (SSSA) ha assegnato un premio al sistema di Ginevra definendolo un eccellente progetto di modernizzazione³³. Anche l'Unione europea ha premiato il sistema di Ginevra due volte, quale finalista nell'ambito dell'eEurope Awards e quale esempio di «Good Practice».

In vista di un perfezionamento, il Cantone di Ginevra sta studiando una nuova soluzione di criptaggio, in grado di proteggere ancora meglio il voto contro eventuali attacchi, dal dispositivo di immissione sino all'urna elettronica. A tal fine deve essere installata un'applicazione nel dispositivo di immissione, senza per questo compromettere la facilità d'uso; l'evoluzione nel settore della sicurezza giustifica un

³² Per la tabella riassuntiva delle prove pilota, cfr. la documentazione complementare 4.

³³ Cfr. comunicato stampa della SSSA del 29 ottobre 2004, www.sgvm.ch/schwerpunkt/archiv/d/dossier8_qualitaetswettbewerb.php.

passo del genere. Inoltre la capacità del sistema viene ampliata affinché in un prossimo futuro tutti gli aventi diritto di voto nel Cantone di Ginevra e gli Svizzeri all'estero con diritto di voto nel Cantone possano utilizzare il voto elettronico.

4.2 Il progetto pilota del Cantone di Neuchâtel

4.2.1 Condizioni quadro

La collaborazione tra la Confederazione e il Cantone di Neuchâtel nell'ambito del progetto voto elettronico è stata regolata nella lettera d'intenti firmata dal nostro Collegio e dal Consiglio di Stato del Cantone di Neuchâtel il 25 aprile 2001 e precisata dettagliatamente nel contratto stipulato tra la Cancelleria federale e la Cancelleria dello Stato del Cantone di Neuchâtel il 18 giugno 2001. Questo contratto disciplina in particolare gli obiettivi del progetto pilota neocastellano e la ripartizione dei costi tra la Confederazione e il Cantone.

L'obiettivo perseguito con il progetto pilota messo in opera nel Cantone di Neuchâtel era di dimostrare che è possibile realizzare un sistema di voto elettronico basato su una struttura di sicurezza a due livelli, analoga a quella di numerosi sistemi esistenti di telebanking: al primo livello, un accesso controllato, consentito dall'identificazione dell'utente, da una parola d'ordine confidenziale e una lista personale di numeri e, al secondo livello, un codice confidenziale personale. Concretamente, gli obiettivi sono stati raggiunti con la progettazione di un voto elettronico integrato nel Guichet Unique, uno sportello virtuale sicuro realizzato dal Cantone di Neuchâtel; il voto elettronico è una delle prestazioni di questo sportello.

4.2.2 Basi legali e condizioni cantonali

Nell'ottobre 2001, il Gran Consiglio neocastellano ha adottato un decreto³⁴ che autorizza il Consiglio di Stato a introdurre il voto elettronico a titolo sperimentale e con riserva dell'accordo della Confederazione, a condizione che la sicurezza del voto e il rispetto del segreto del voto siano garantiti e che i rischi di frodi e di abusi siano esclusi (art. 4).

Nel settembre 2002, la revisione³⁵ della legge cantonale sui diritti politici ha permesso di introdurre la nuova organizzazione degli scrutini. I principali cambiamenti sono la costituzione di un archivio centrale degli elettori prima di ogni scrutinio (art. 6e), la stampa e la distribuzione del materiale di voto in modo centralizzato (art. 6f e 9a) e la creazione di una carta di legittimazione unica per elettore e per scrutinio che integra le informazioni necessarie per il voto per corrispondenza e per il voto elettronico e che serve da legittimazione per il voto tradizionale (art. 9). Questo nuovo sistema permette ai Comuni e al Cantone di gestire con facilità uno scrutinio realizzato con diverse modalità di voto (all'urna, per corrispondenza e via Internet) e di controllare che gli elettori votino una sola volta.

³⁴ Décret sur l'introduction à titre expérimental des moyens électroniques facilitant l'exercice des droits politiques du 3 octobre 2001 (Recueil systématique de la législation neuchâteloise 141.03).

³⁵ Loi du 4 septembre 2002 portant révision de la loi sur les droits politiques (Feuille officielle no 68 du 13 septembre 2002, pages 990 à 992).

Nel settembre 2004, il Gran Consiglio neocastellano ha adottato la legge sul Guichet Unique³⁶, il cui scopo è di definire le condizioni di organizzazione, esercizio e impiego del Guichet Unique. Questa legge definisce in particolare le procedure attraverso le quali sono forniti i diritti d'accesso (art. 10, 18 e 19) come pure i differenti aspetti relativi alla sicurezza del Guichet Unique (art. 13–17) e alla protezione dei dati (art. 23–25). La legge concerne anche il voto elettronico nella misura in cui è stato sviluppato nell'ambito del Guichet Unique.

4.2.3 Soluzione e realizzazione

4.2.3.1 Voto elettronico integrato nel Guichet Unique

Nel Cantone di Neuchâtel, il voto elettronico era integrato sin dall'inizio in un progetto più vasto finalizzato all'elaborazione di uno sportello virtuale sicuro, che offrisse agli abitanti del Cantone una scelta di prestazioni diverse, tra cui il voto via Internet. In cooperazione con le società Computer Associates e Lanexpert, il Cantone ha pertanto realizzato il Guichet Unique, per offrire un nuovo mezzo di comunicazione e di transazione tra le collettività pubbliche neocastellane e i loro utilizzatori (elettori, contribuenti, proprietari ecc.) e clienti (imprese e mandatari). Il Guichet Unique permette di ricevere prestazioni e di scambiare in piena sicurezza dati confidenziali tra partner del settore pubblico e privato.

A disposizione del pubblico dal 5 maggio 2005, il Guichet Unique³⁷ offre servizi nell'ambito della fiscalità (consultazione dei conti correnti fiscali, delle notifiche di tassazione, dei termini di pagamento, dei calcoli delle rate fiscali ecc.) e della mobilità (ricerca di detentori di targhe). Il voto elettronico è stato sperimentato per la prima volta nell'ambito di una votazione ufficiale in occasione dello scrutinio federale del 25 settembre 2005. Questa soluzione di voto elettronico è stata elaborata in collaborazione con partner privati, tra cui principalmente Arcantel (per l'applicazione) e Scytl (per il criptaggio).

Per poter votare on line, gli elettori del Cantone di Neuchâtel devono iscriversi al Guichet Unique compilando un modulo di adesione e legalizzando la loro firma presso un'autorità competente (Cancelleria dello Stato, amministrazioni comunali, registri dei tribunali distrettuali o notai abilitati). La Cancelleria dello Stato del Cantone di Neuchâtel controlla questi dati prima di definire i parametri del conto di un utente. L'utente riceve quindi, con posta separata, un codice d'utente e una parola d'ordine, come pure, in un secondo tempo, la lista di numeri. Dopo aver modificato la parola d'ordine in occasione del primo collegamento, l'utente può accedere alle differenti prestazioni del Guichet Unique. L'utente riceve anche il materiale e il supporto necessari per aggiornare la sua postazione e renderla compatibile con il Guichet Unique.

Se beneficia dei diritti di voto nel Cantone di Neuchâtel, prima dello scrutinio l'utente riceve la sua carta di legittimazione che gli consente di votare, a scelta, all'urna, per corrispondenza o via Internet. La carta contiene un codice di validazione e un codice di conferma confidenziali, destinati specificamente al voto on line.

³⁶ Loi du 28 septembre 2004 sur le guichet sécurisé unique (LGSU) (Feuille officielle n° 80 du 15 octobre 2004, pages 1205 à 1207).

³⁷ Cfr. www.guichetunique.ch

Al momento di votare, l'utente apre il proprio conto presso il Guichet Unique e si identifica come per qualsiasi altra prestazione. Successivamente accede allo scrutinio, secondo i suoi diritti di voto (ad esempio, una persona con il permesso C può accedere solo agli scrutini cantonali o comunali) e può esprimere le sue preferenze contrassegnando le corrispondenti caselle sulle schede di voto elettroniche. Il sistema presenta quindi una ricapitolazione delle risposte; se è soddisfatto delle scelte, il votante immette il codice di validazione che figura sulla sua carta di legittimazione. A questo punto il voto è espresso e appaiono allo schermo il codice di conferma (che figura anche sulla carta di legittimazione) e un codice denominato «accusé de réception» (avviso di ricevimento). Il codice di conferma permette di verificare immediatamente, confrontandolo con il codice registrato sulla scheda, che il voto è stato ricevuto dal server del voto elettronico neocastellano. L'avviso di ricevimento prova invece che il voto è giunto nell'urna. Dopo la chiusura dello scrutinio e lo spoglio dell'urna elettronica il votante può verificare che il suo avviso di ricevimento figuri nella lista pubblicata su Internet; se lo trova, ha la conferma che il suo voto è stato preso in considerazione al momento dello spoglio. L'avviso non è legato al voto stesso, ma al certificato elettronico che lo accompagna. Sulla base di questo avviso non è dunque possibile conoscere il voto espresso da una persona.

La sicurezza e il rispetto del segreto del voto sono garantiti dal fatto che il voto è criptato dall'inizio alla fine cioè dal momento in cui è espresso sulla postazione cliente fino alla sua registrazione nell'urna. L'architettura fisica del Guichet Unique e del voto elettronico è salvaguardata in locali ad alta sicurezza, il cui accesso è autorizzato solo a persone giurate.

4.2.3.2 Nuova organizzazione degli scrutini

A livello organizzativo, il sistema di voto elettronico attraverso il Guichet Unique è parte della nuova organizzazione generale degli scrutini, in vigore da maggio 2003. Prima di ogni scrutinio, i registri comunali sono trasferiti nell'infrastruttura del Guichet Unique. Sulla base di questi 62 archivi comunali, viene costituito un catalogo centrale degli elettori.

Il catalogo centrale permette di garantire l'unicità del voto, perché la prima registrazione di un voto blocca le altre modalità. Le carte di legittimazione sono infatti controllate in base a un codice a barre stampato sulla carta. Se risulta che l'elettore ha già votato via Internet, sono esclusi il voto per corrispondenza e quello all'urna; se ha già votato per corrispondenza, l'elettore non potrà più accedere allo scrutinio elettronico attraverso il Guichet Unique.

Dopo la creazione del catalogo centrale, sono generati le carte di legittimazione e il catalogo degli elettori che dispongono di un accesso al Guichet Unique e possono votare elettronicamente. Durante questo processo sono creati anche i codici di validazione e di conferma stampati sulle carte di legittimazione. Le carte di legittimazione sono quindi trasferite alla tipografia cantonale per la stampa. Per motivi di sicurezza, sulla carta utilizzata è riprodotto un ologramma con lo stemma del Cantone di Neuchâtel.

4.2.3.3 Processo di voto elettronico

Il processo di voto elettronico comincia con l'attribuzione dei parametri all'urna elettronica, che può aver luogo solo alla presenza della commissione elettorale, composta di cinque deputati del Gran Consiglio, del Cancelliere dello Stato e di un giurista. I membri di questa commissione sorvegliano le differenti tappe del processo, di cui fa parte anche la generazione della chiave pubblica e della chiave privata. La chiave pubblica serve per criptare i voti elettronici direttamente sulle postazioni dei votanti. La chiave privata consente invece di decriptare i voti dopo la chiusura dello scrutinio. Al momento dell'attribuzione dei parametri, la chiave privata è suddivisa in due parti e registrata su smart card distribuite a un numero predefinito di membri della commissione elettorale. Questi proteggono l'accesso alle loro smart card registrando una parola d'ordine prima di depositare il tutto in buste sigillate.

Per assicurarsi che il sistema di voto funzioni correttamente e che il contenuto dell'urna elettronica non sia manipolato, ogni membro della commissione elettorale si collega al Guichet Unique, vota e stampa l'avviso di ricevimento. Ogni voto è notificato e depositato in una busta sigillata con l'avviso di ricevimento.

Le parole d'ordine, le smart card con la chiave privata per la decriptazione dei voti, le postazioni di lavoro (portatili) e i voti della commissione sono conservati in locali protetti (Polizia cantonale e cassaforte della Cancelleria dello Stato).

Per lo spoglio dei voti elettronici il giorno dello scrutinio, la commissione elettorale si riunisce nuovamente e raccoglie tutto il materiale (postazioni di lavoro e buste sigillate) portato indietro dalla Cancelleria dello Stato e dalla Polizia cantonale.

I membri della commissione elettorale recuperano le smart card, immettono le loro parole d'ordine e sbloccano la chiave privata per decriptare i voti. Dopo essere stati decriptati, i voti e gli avvisi di ricevimento sono estratti e mescolati. Un programma permette di validare i voti e di contarli. La validazione permette di verificare la struttura delle schede di voto e i diritti di voto degli elettori e di scartare i voti errati e quelli fraudolenti.

I membri della commissione elettorale verificano quindi la correttezza dei loro voti facendo un confronto tra i risultati dell'urna e le schede depositate nelle buste sigillate.

La Cancelleria dello Stato redige un verbale che contiene una validazione di tutte le tappe e di tutte le decisioni e comunica i risultati del voto elettronico ai Comuni. Dopo il termine legale di ricorso, le informazioni sono conservate fino al momento in cui il Consiglio federale valida definitivamente il risultato della votazione sul piano nazionale. Successivamente, le schede di voto sono distrutte e i supporti di dati cancellati.

4.2.4 Prove pilota e lavori collaterali

4.2.4.1 Prove pilota e audit di sicurezza

Dopo una fase di sviluppo di due anni, il primo test di voto elettronico è stato eseguito nel gennaio 2005, con un gruppo di 336 «votanti elettronici» dell'amministrazione cantonale neocastellana, della Cancelleria federale e del gruppo di monitoraggio. Questo test su piccola scala ha consentito di verificare il funzionamento del

sistema e di determinare i punti da migliorare a livello di ergonomia e di compatibilità con le configurazioni informatiche esistenti. Il test ha fornito buoni risultati e i suggerimenti dei collaudatori sono stati presi in considerazione.

Le seconda prova di voto elettronico si è svolta nel febbraio 2005 con le stesse persone, per collaudare il funzionamento dei miglioramenti apportati al sistema. Dopo il successo di questo test, il Cantone di Neuchâtel ha messo in opera, nel marzo 2005, un terzo test in grandezza reale, sempre nell'ambito di una votazione fittizia, con almeno 2600 «votanti», scelti tra i collaboratori dell'amministrazione federale, cantonale e comunale. Dato che il voto elettronico neocastellano è legato al Guichet Unique, non era possibile organizzare una prova con una votazione ufficiale comunale. A un determinato numero di collaudatori è stata data la possibilità di votare via Internet e per corrispondenza, per verificare l'interoperabilità dei differenti canali di voto. La società blue-infinity incaricata dell'audit esterno ha ricevuto dal Cantone di Neuchâtel e dalla Cancelleria federale l'incarico di esaminare la sicurezza del sistema di voto elettronico, in particolare provando ad attaccarlo durante il periodo della sperimentazione. La commissione elettorale ha assistito all'apertura e alla chiusura dell'urna elettronica, come nel caso di una votazione reale.

A livello di organizzazione e svolgimento dello scrutinio il terzo test si è svolto senza problemi. Per i 2600 partecipanti sono stati creati conti di Guichet Unique; il materiale di voto (via Internet e per corrispondenza) e i diversi documenti esplicativi sono stati distribuiti per posta. Hanno votato 1463 persone, di cui 1458 via Internet. I voti spediti in doppio – via Internet e per corrispondenza – sono stati scoperti e scartati dal sistema. La società di audit è riuscita a modificare il contenuto di 20 voti, prima del loro criptaggio e invio nell'urna elettronica, che il Cantone di Neuchâtel le aveva fornito per scopi di prova. Di conseguenza, il successo di questo test è stato considerato solo parzialmente raggiunto. Seguendo le raccomandazioni della società di audit alla fine del test, il Cantone di Neuchâtel ha intrapreso i lavori necessari per consolidare il sistema.

Successivamente, il Cantone di Neuchâtel e la Cancelleria federale hanno deciso che si doveva procedere a un quarto test su piccola scala, nell'aprile 2005, per verificare l'efficacia delle misure di consolidamento. La stessa società di audit è stata incaricata di verificare la validità delle misure di sicurezza, cercando nuovamente di attaccare il sistema. Questa volta la prova si è svolta senza problemi, con 420 voti espressi, e i collaudatori hanno potuto constatare che i difetti del sistema erano stati eliminati.

Parallelamente, durante i mesi di dicembre 2004 e gennaio 2005, la sicurezza del Guichet Unique è stata sottoposta a verifica dalla società PriceWaterhouse&Coopers, su incarico del dipartimento delle finanze del Cantone di Neuchâtel. Nel corso delle loro analisi, i collaudatori hanno potuto individuare difetti di sicurezza a livello di processo di autenticazione. Questi difetti sono stati quindi efficacemente corretti. Nel maggio 2005, il Cantone di Neuchâtel ha potuto consegnare alla Cancelleria federale un documento ufficiale attestante che i problemi di sicurezza emersi durante le verifiche in materia di Guichet Unique e voto elettronico erano risolti.

Convinto che il sistema aveva raggiunto il livello di maturità e di sicurezza necessario per essere sperimentato nell'ambito di una votazione ufficiale, il Cantone di Neuchâtel ha presentato al nostro Collegio, nell'aprile 2005, la domanda per svolgere una prova pilota di voto elettronico nell'ambito dello scrutinio federale del 25 settembre 2005, proponendo di limitare il numero dei partecipanti alle prime

2000 persone iscritte al Guichet Unique. Il 22 giugno 2005 abbiamo dato l'accordo; 1178 elettori, cioè il 68,0 per cento dei votanti che avevano la possibilità di partecipare a questo scrutinio, hanno espresso il voto attraverso il loro conto di Guichet Unique. Il primo test ufficiale si è svolto senza problemi. I risultati del questionario on line proposto ai votanti indicano che il sistema di voto elettronico neocastellano è apprezzato dagli utenti³⁸.

Nell'agosto 2005, il Cantone di Neuchâtel ha inoltrato la domanda per svolgere una seconda prova pilota nell'ambito dello scrutinio federale del 27 novembre 2005. Delle 2442 persone che hanno stipulato un contratto per il Guichet Unique (il 55,08 %) 1345 elettori hanno espresso il voto attraverso il loro conto presso il Guichet Unique; ciò corrisponde al 2,5 per cento dei voti espressi nel Cantone di Neuchâtel.

Nel frattempo, il Cantone di Neuchâtel ha organizzato anche un'elezione suppletiva al Consiglio degli Stati. Il primo turno si è svolto il 30 ottobre 2005 con quattro candidati che si presentavano per occupare il seggio lasciato vacante da Jean Studer. Nell'urna sono stati depositati 1194 voti elettronici, che corrispondono al 54 per cento degli elettori che dispongono di un accesso al Guichet Unique³⁹.

Nel corso delle tre prove di voto elettronico (votazioni popolari ed elezione), lo svolgimento delle procedure di preparazione e di spoglio dell'urna elettronica non è stato disturbato da inconvenienti. Tutte le procedure sono state eseguite secondo quanto definito e pianificato.

4.2.4.2 Lavori collaterali

Come i progetti pilota di Ginevra e di Zurigo, anche quello neocastellano è seguito sin dall'inizio da un gruppo specifico, coordinato dalla Cancelleria federale e composto di rappresentanti della Confederazione e dei Cantoni. Compito di questo gruppo è valutare il progetto recandosi sul posto per assistere alle tappe importanti. Le attività e le rilevazioni del gruppo sono presentate regolarmente in rapporti messi a disposizione della Cancelleria federale.

Durante l'anno 2003, il gruppo di monitoraggio ha seguito l'attuazione della nuova organizzazione degli scrutini del Cantone di Neuchâtel, verificando i processi chiave come la creazione del catalogo centrale degli elettori, la gestione degli errori nel registro e lo spoglio dei suffragi espressi nella votazione del 18 maggio 2003. Durante gli anni 2004 e 2005, il gruppo ha assistito alle differenti tappe della realizzazione del voto elettronico neocastellano. I suoi membri hanno ricevuto le informazioni necessarie per valutare il sistema di voto elettronico, hanno partecipato all'apertura e alla chiusura dell'urna, ai test nella veste di «votanti» e ai rapporti in materia di audit di sicurezza. Secondo il gruppo, la collaborazione con il team del progetto neocastellano si è svolta in modo efficace e trasparente. Basandosi sulle sue rilevazioni, il gruppo di monitoraggio si è espresso favorevolmente quando il Cantone di Neuchâtel ha presentato le domande per svolgere i suoi primi test ufficiali di voto elettronico in occasione delle votazioni federali del 25 settembre e del 27 novembre 2005. Inoltre ha assistito come osservatore ai differenti processi di

³⁸ Cfr. n 5.1.2.2

³⁹ Per la tabella riassuntiva delle prove pilota, cfr. la documentazione complementare 4.

questi test ufficiali e ha potuto rendersi conto del corretto svolgimento delle operazioni.

4.3 Il progetto pilota del Cantone di Zurigo

4.3.1 Condizioni quadro

La dichiarazione di intenti «Procedura di votazione ed elezione con mezzi tecnici» tra il nostro Collegio e il Consiglio dello Stato del Cantone di Zurigo è stata firmata rispettivamente il 7 e il 17 dicembre 2001.

La dichiarazione di intenti è servita da base per il contratto stipulato il 25 gennaio/1° febbraio 2002 tra la Cancelleria federale svizzera e la Direzione della Giustizia e degli Interni del Cantone di Zurigo, in cui sono stati definiti tra l'altro i seguenti obiettivi:

- realizzazione di un catalogo elettorale cantonale sulla base dei dati estratti dai cataloghi locali degli abitanti e dai cataloghi elettorali dei 171 Comuni del Cantone di Zurigo;
- realizzazione di un vasto sistema di votazione ed elezione elettronico;
- qualità di mandatario a tutti gli effetti, che consente ai Comuni di svolgere votazioni ed elezioni comunali su base elettronica;
- diversi dispositivi di immissione per l'esercizio del diritto di partecipare alle elezioni e votazioni.

4.3.2 Basi legali e condizioni cantonali

L'impiego del voto elettronico è regolato nella legge cantonale sui diritti politici (Gesetz über die politischen Rechte [GPR]) del 1° settembre 2003. Secondo l'articolo 4 capoverso 2 di questa legge «essi [i diritti politici] possono essere esercitati per via elettronica, se sono soddisfatte le premesse tecniche e organizzative. La volontà degli aventi diritto di voto deve essere appurata in modo corretto e il segreto del voto deve essere garantito».

A complemento della legge cantonale è stata emanata l'ordinanza cantonale sui diritti politici del 27 ottobre 2004, che non si occupa tuttavia esplicitamente di votazioni ed elezioni elettroniche. All'articolo 12 menziona solo che per prove di voto elettronico si può derogare all'ordinanza e che il Consiglio dello Stato del Cantone di Zurigo disciplina le misure necessarie.

4.3.3 Soluzione e realizzazione

Il Cantone di Zurigo dispone di cataloghi elettorali gestiti in maniera completamente decentralizzata. Ognuno dei 171 Comuni zurighesi è responsabile della gestione e dell'aggiornamento del proprio catalogo elettorale.

Per questo motivo, nel Cantone di Zurigo è stato sviluppato un sistema che consente ai Comuni di continuare a gestire i propri cataloghi elettorali in modo autonomo.

Il sistema di Zurigo è stato realizzato per votazioni popolari semplici, per iniziative con controprogetto e domanda risolutiva, come pure per elezioni secondo il sistema maggioritario e secondo il sistema proporzionale. In caso di elezioni secondo il sistema maggioritario sono possibili sia elezioni con candidati precedentemente annunciati sia elezioni con candidati non annunciati, nell'ambito delle quali sono eleggibili tutti gli aventi diritto di voto passivi cioè, a seconda della base legale, anche persone senza domicilio politico nel Cantone di Zurigo.

Secondo la legge, nel Cantone di Zurigo spetta ai Comuni fissare l'orario di apertura delle urne; nel configurare il sistema se ne è tenuto conto. Prima di ogni votazione si può fissare per ogni Comune l'ora della chiusura dell'urna elettronica. A quest'ora individuale l'urna elettronica viene chiusa automaticamente.

Anche il criptaggio dei voti è effettuato per Comune. Le parole d'ordine necessarie per decrittare i voti la domenica della votazione sono spediti per posta ai responsabili delle elezioni e delle votazioni.

Per impedire che si possa votare più volte sono stati integrati diversi meccanismi di controllo. Da ogni seggio elettorale si può accedere direttamente al modulo di controllo del sistema mediante collegamento on line oppure svolgere il controllo mediante un apparecchio di lettura del codice a barre. Lo stesso controllo può essere effettuato però anche in modalità off line; i documenti di voto dubbi sono trasferiti dal seggio elettorale all'ufficio elettorale del Comune dove vengono controllati on line. In caso di necessità, per la verifica nel seggio elettorale possono essere utilizzate anche liste di controllo stampate.

Il sistema di Zurigo è un sistema completamente integrato. Prima dell'inizio della votazione, i risultati dei lavori di preparazione compresi i documenti di voto e i circondari elettorali sono esportati dal sistema di votazione ed elezione WABSTI e trasferiti nel sistema di voto elettronico. Dopo la chiusura dell'urna elettronica e fisica, si possono nuovamente esportare tutti i dati della votazione nel sistema WABSTI semplicemente premendo un tasto; i voti sono sommati a quelli espressi per corrispondenza e a quelli depositati nelle urne nei seggi elettorali. In questo modo, dati precedentemente convalidati sono elaborati direttamente on line attraverso un'interfaccia. Questo procedimento sostiene notevolmente l'economicità del voto elettronico. I dati provenienti dall'urna elettronica, anche i voti ottenuti con il panache e il cumulo, possono essere attribuiti automaticamente e correttamente nel sistema di base.

Oltre alla possibilità di votare elettronicamente per Internet, il Cantone di Zurigo ha sviluppato un modulo per votare con il telefono cellulare (SMS). Nel Cantone di Zurigo si possono anche svolgere elezioni con i mezzi elettronici menzionati precedentemente. L'apposito modulo è stato testato efficacemente alla fine del 2004 in occasione delle elezioni del consiglio degli studenti dell'Università di Zurigo. La società SwissICT e la rivista InfoWeek hanno premiato il sistema di Zurigo nel settembre 2005 conferendogli lo Swiss IT Award 2005 per il miglior software dell'anno⁴⁰.

⁴⁰ Cfr. comunicato stampa del 15 settembre 2005 della Direzione della Giustizia e degli Interni del Cantone di Zurigo.

4.3.3.1

Una votazione con il voto elettronico

Gli aventi diritto di voto possono scegliere se votare elettronicamente, per corrispondenza o recandosi alle urne. Tutte le indicazioni necessarie per le singole possibilità si trovano sulla carta di legittimazione che gli aventi diritto di voto ricevono per posta prima di ogni votazione.

La votazione comincia con l'esportazione nel catalogo elettorale virtuale dei cataloghi elettorali comunali decentralizzati. Non appena il catalogo è completo vengono prodotte e stampate le carte di legittimazione al voto. Contemporaneamente sono generati anche i codici di accesso individuali che vengono stampati sulle carte di legittimazione. Dopo la stampa delle carte di legittimazione, i dati personali sono cancellati dal catalogo elettorale virtuale. Da questo momento non si possono più stabilire nessi tra voti e persone e il segreto di voto è garantito in ogni momento.

Il giorno prestabilito, l'urna elettronica viene aperta. Per essere sicuri che il sistema funziona correttamente, i rappresentanti della centrale di votazione esprimono voti verbalizzati per un Comune fittizio. Questi voti sono controllati al momento della determinazione dei risultati.

Gli aventi diritto di voto si annunciano al sistema di voto elettronico con il codice di accesso stampato sulla carta di legittimazione. Quindi possono esprimere le proprie preferenze in merito ai testi per i quali sono legittimati (le persone che poco prima di una votazione trasferiscono il domicilio in un altro Comune del Cantone, ad esempio, per un determinato periodo di tempo non hanno diritto di voto nel nuovo Comune di domicilio; devono invece poter esercitare il loro diritto di voto a livello federale e cantonale). In Internet i votanti esprimono il voto compilando gli appositi campi. Al termine di questa operazione il sistema mostra ancora una volta ai votanti le loro scelte affinché possano fare un ultimo controllo, prima della conferma definitiva. Dopo la conferma, i voti sono memorizzati definitivamente nell'urna elettronica.

Il Cantone di Zurigo ha previsto quale ulteriore possibilità di esprimere il voto oltre a Internet anche la telefonia mobile (SMS). Gli elettori dispongono in linea di principio delle stesse varianti di votazione ed elezione come via Internet. Per poter garantire il segreto anche in caso di voto con SMS, a ogni avente diritto di voto viene inviato sulla carta di legittimazione una tabella individuale di codici. L'immissione delle caratteristiche di voto avviene tramite SMS in forma precodificata. Invece di sì, no o scheda bianca sono introdotti nell'apparecchio di immissione corrispondenti codici di quattro posizioni. Per l'identificazione è necessario il numero di identificazione d'utente che si trova sulla carta di legittimazione. I voti così definiti giungono nell'urna elettronica attraverso il gateway SMS proprio del sistema e dopo un controllo automatico della legittimazione.

Per esprimere il voto sono spediti al gateway con il numero di destinazione 28000 uno o, in caso di elezioni, eventualmente più messaggi SMS corrispondenti. Il sistema esige quindi l'immissione di ulteriori dati per l'autenticazione del voto. A tal fine occorre un codice PIN che, protetto da un sigillo di sicurezza, è integrato nella carta di legittimazione. Inoltre è necessario indicare la corretta data di nascita. Dopo aver votato, la persona avente diritto di voto riceve una conferma SMS conclusiva del corretto svolgimento dell'operazione di voto.

In entrambi i media (Internet e SMS) i voti sono pertanto già criptati sull'apparecchio di immissione. La decriptazione avviene solo dopo la chiusura di tutte le urne (fisiche ed elettroniche), affinché si possa procedere allo spoglio. Dopo la decriptazione di tutti i voti è determinato il risultato totale. Dapprima i voti verbalizzati espressi per un Comune virtuale sono contati e confrontati con i verbali. Solo se i verbali e i risultati dello spoglio concordano si può presumere che il sistema abbia funzionato correttamente. Quindi i voti elettronici ricevuti sono trasmessi al sistema di analisi WABSTI e sommati ai voti ricevuti in maniera convenzionale e infine viene determinato il risultato complessivo (totale dei voti elettronici e dei voti convenzionali). Naturalmente i voti di prova del Comune virtuale espressi dalla centrale di voto non sono inclusi nel risultato finale.

4.3.4 Prove pilota e lavori collaterali

Il Cantone di Zurigo ha svolto sinora quattro test; in occasione del primo e dell'ultimo non hanno avuto luogo votazioni, ma elezioni in base al sistema proporzionale.

In occasione delle elezioni 2004 del consiglio degli studenti dell'Università di Zurigo, il Cantone di Zurigo ha potuto sperimentare per la prima volta una parte (modulo dell'elezione secondo il sistema proporzionale) della sua soluzione di voto elettronico. Il test è stato coronato da successo. Solo al momento del trasferimento al WABSTI sono sorti alcuni piccoli problemi tecnici, non essendo ancora disponibile l'interfaccia. I problemi sono stati tuttavia superati grazie al rilevamento manuale dei voti depositati nell'urna elettronica.

Dei 24 000 studenti aventi diritto di voto, 2188 hanno partecipato alle elezioni, con una quota di partecipazione del 9,11 per cento, superiore di quasi il 100 per cento a quella delle precedenti elezioni del consiglio degli studenti, che non prevedevano la possibilità di votare elettronicamente. 1610 persone, cioè il 73,6 per cento, hanno utilizzato Internet; 429 persone, ossia il 19,6 per cento, hanno votato per SMS e 149, (il 6,8 %) all'urna.

Rappresentanti della Cancelleria federale e del gruppo di monitoraggio Zurigo hanno potuto assistere sia all'apertura dell'urna che allo spoglio dei voti ricevuti elettronicamente e confermare al Cantone di Zurigo lo svolgimento corretto delle elezioni.

Unisys, l'impresa generale incaricata di sviluppare la soluzione zurighese di voto elettronico, ha eseguito vasti test interni nella primavera 2005. I test sono stati realizzati con l'ausilio di un robot sviluppato dalla Unisys, che generava e verbalizzava voti casuali basati su un algoritmo.

I test hanno evidenziato alcune lacune che secondo la ditta Unisys non sarebbero state scoperte se i voti fossero stati immessi manualmente. Le lacune sono state eliminate dall'impresa generale immediatamente dopo l'ultimazione dei test.

L'audit del sistema e l'audit interno della sicurezza sono stati svolti dalla ditta Swisscom solutions.

Su richiesta del gruppo di monitoraggio e d'intesa con il Cantone di Zurigo, la Cancelleria federale svizzera ha incaricato una ditta indipendente di condurre un audit interno della sicurezza. La ditta blue-infinity con sede a Ginevra ha già effet-

tuato audit simili nei Cantoni pilota di Ginevra e Neuchâtel e disponeva pertanto dell'esperienza necessaria in questo ambito.

L'audit è stato eseguito dal 18 luglio 2005 al 7 agosto 2005 e ha evidenziato i seguenti potenziali di miglioramento:

- i file di aiuto che possono essere richiamati dai votanti per ricevere assistenza erano installati su un server non sufficientemente protetto, esterno alla soluzione zurighese di voto elettronico;
- la schermata con la quale i voti sono presentati ai votanti sul mezzo di immissione era troppo poco affidabile;
- la lunghezza delle parole d'ordine (otto segni alfanumerici) dovrebbe essere aumentata.

Il Cantone di Zurigo e la Unisys Svizzera SA hanno corretto i due primi punti già per i due test del 30 ottobre 2005 (votazione comunale a Bülach) e del 27 novembre 2005 (votazione federale/cantonale). Per motivi di usabilità, il previsto adeguamento della lunghezza delle parole d'ordine da otto a 16 segni non è stato ancora realizzato; sarà comunque intrapreso a medio termine.

Il primo test del modulo di votazione è stato svolto il 30 ottobre 2005 nella città di Bülach. A 9443 persone aventi diritto di voto è stata offerta la possibilità di utilizzare i media elettronici (Internet, Natel).

Ha partecipato al voto il 41,49 per cento degli aventi diritto, il 37,27 per cento dei quali per via elettronica. 1006 voti sono stati espressi via Internet e 455 voti con il telefono cellulare.

Il test è stato seguito e controllato da membri del gruppo di monitoraggio di Zurigo. Non è stata riscontrata nessuna irregolarità.

A livello federale, il sistema zurighese di voto elettronico è stato sperimentato la prima volta il 27 novembre 2005. La prova si è svolta nei Comuni di Bertschikon, Bülach e Schlieren (16 726 aventi diritto di voto). Nei tre Comuni è stata registrata una partecipazione al voto del 37,72 per cento (6310 persone).

Dei 6310 votanti, 1397 (il 22,14 %) hanno deciso di votare per via elettronica. Di questi, l'82,61 per cento (1154 persone) ha votato via Internet e il 17,39 per cento (243 persone) tramite SMS.

A Bertschikon, un piccolo Comune rurale, il 43 per cento dei votanti è ricorso al voto elettronico. Dei votanti per via elettronica il 37,2 per cento (58 voti) ha utilizzato SMS e il 62,8 per cento (98 voti) Internet. La prova pilota è stata controllata da rappresentanti della Cancelleria federale⁴¹.

Dopo il 2004 il sistema di Zurigo è stato impiegato ancora nel dicembre 2005 per le elezioni del consiglio degli studenti dell'Università di Zurigo. Dei 23 096 studenti aventi diritto di voto, 1767 hanno partecipato alle elezioni, con una quota di partecipazione del 7,7 per cento. 1582 persone, cioè l'88,5 per cento, hanno utilizzato Internet; 205 persone, ossia l'11,4 per cento, hanno votato per SMS. Una sola persona ha votato all'urna (0,1 %). Per contare i voti e determinare i risultati, con più dell'80 per cento di schede elettorali modificate, ci sono voluti 18 minuti.

⁴¹ Per la tabella riassuntiva delle prove pilota, cfr. la documentazione complementare 4.

Al termine dei lavori di valutazione erano a disposizione anche i risultati delle prime elezioni politiche con voto elettronico secondo il sistema proporzionale. Il 2 aprile 2006 i cittadini del Comune di Bülach hanno eletto il loro consiglio comunale (elezioni secondo il sistema maggioritario) e il loro Municipio (elezioni secondo il sistema proporzionale). Il 20,67 per cento degli elettori ha votato per via elettronica. Dei 728 voti elettronici 28 (il 3,85 %) sono giunti per SMS.

4.3.4.1 Lavori collaterali

Nell'ambito del suo mandato, la Cancelleria federale svizzera ha incaricato gruppi di monitoraggio di seguire i tre progetti pilota. Fra i compiti del gruppo di monitoraggio di Zurigo figuravano il controllo dell'organizzazione del progetto (organizzazione e svolgimento, verifica dei rapporti sui progressi), la comunicazione di informazioni rilevanti sul progetto di Zurigo al «gruppo di lavoro voto elettronico» della Cancelleria federale svizzera, la valutazione dei concetti tecnici, il monitoraggio di audit di sistema, la valutazione e la verifica del rispetto delle direttive in materia di protezione dei dati come pure la presentazione al Consiglio federale di raccomandazioni in relazione con domande di prove di voto elettronico in occasione di votazioni federali.

4.4 Progetti di altri Stati⁴²

Il voto elettronico nel seggio elettorale è già stato utilizzato su vasta scala per elezioni nazionali in Belgio, Paesi Bassi⁴³, negli USA, in Russia, Azerbaigian, Brasile, Paraguay e India e per casi singoli e prove pilota ad esempio anche in Germania, Canada, Portogallo, Danimarca e Australia. In Irlanda, Portogallo, Finlandia, Kazakistan, Canada, Messico, Corea, Venezuela, Perù e Colombia l'introduzione di macchine di voto è allo studio.

Il voto elettronico via Internet viene invece sperimentato in numerosi Stati nell'ambito di progetti pilota regionali. In molti Paesi si svolgono inoltre già via Internet elezioni non politiche in istituzioni di diritto pubblico (p. es. elezioni del consiglio degli studenti o elezioni dei consigli aziendali). A parte l'Estonia, nessuno Stato sovrano ha comunque introdotto definitivamente il voto elettronico via Internet per elezioni o votazioni giuridicamente vincolanti (referendum).

Negli ultimi anni sono state effettuate elezioni giuridicamente vincolanti in Gran Bretagna (elezioni regionali 2002 e 2003), Giappone (a livello comunale dal 2003), Paesi Bassi (elezioni del Parlamento dell'Unione europea 2004 con gli Olandesi all'estero), Spagna (referendum locale 2004), Francia (elezione dell'Assemblea dei Francesi all'estero 2006), Canada (elezioni locali in Ontario 2003).

⁴² Cfr. Österreichisches Bundesministerium des Innern (Ministero federale austriaco dell'interno), Bericht der Arbeitsgruppe E-Voting, Internationaler Teil (rapporto del gruppo di lavoro e-voting, parte internazionale), Vienna 20 ottobre 2004 (www.wahlinfo-bmaa.at/up-media/1137_uagintbericht2010w.pdf). Una tabella non esaustiva delle prove pilota di voto elettronico all'estero è contenuta nella documentazione complementare 10.

⁴³ Dal 1974. Nelle elezioni parlamentari del maggio 2002, il 95 % di tutti i Comuni ha utilizzato macchine di voto elettroniche.

Inoltre in alcuni Paesi e alcune regioni – Austria⁴⁴, Francia⁴⁵, Italia⁴⁶, Catalogna, Spagna⁴⁷, Germania⁴⁸ e Portogallo – sono stati eseguiti test non vincolanti nel settore statale o privato. La Slovenia, l'Ungheria e la Bulgaria dispongono di progetti in forma di disegni di legge non ancora approvati dal Parlamento. La Repubblica Ceca e la Romania hanno comunicato che effettueranno test. Nel Canada, una legge autorizza lo svolgimento di studi e sperimentazioni. L'Austria, la Svezia, la Norvegia, il Lussemburgo e la Bulgaria hanno costituito commissioni politiche che si occupano delle questioni relative al voto elettronico.

In molti Paesi infine le riflessioni e le attività in materia di voto elettronico sono legate a iniziative nell'ambito del Governo elettronico. Il coordinamento soprannazionale, ad es. nel quadro del piano di azione eEurope dell'UE con studi comparativi⁴⁹ concernenti tutti gli Stati membri, assume un ruolo sempre più importante nell'ambito del Governo elettronico e del voto elettronico. Un altro ambito connesso con il voto elettronico è lo sviluppo di un'identità elettronica. Anche a questo proposito vi sono molte convenzioni multilaterali, ad es. dell'UE⁵⁰, già applicate mediante legge e ordinanza in alcuni Stati membri⁵¹.

Inoltre vi è una serie di pubblicazioni scientifiche su diversi aspetti del voto elettronico. Molte di loro hanno raggiunto una risonanza pubblica o privata tale che hanno portato all'abbandono di progetti di voto elettronico (USA, Irlanda)⁵².

La Svizzera ha optato per una velocità moderata e un approccio prudente alla tematica. La fase pilota le ha permesso di fare una valutazione precisa delle applicazioni a livello cantonale e di tenere regolarmente conto delle esperienze all'estero.

4.4.1 Consiglio d'Europa e OSCE

Diversamente da altre organizzazioni internazionali, il Consiglio d'Europa si è occupato intensamente della questione del voto elettronico. Su iniziativa di alcuni dei suoi Stati membri, il Comitato dei ministri ha istituito un gruppo di esperti e adottato il 30 settembre 2004 una Raccomandazione sulle norme giuridiche, tecniche e organizzative del voto elettronico. La Svizzera ha potuto far confluire nell'elaborazione degli standard le esperienze fatte con il voto elettronico. In virtù delle differenti regolamentazioni giuridiche in materia di votazioni ed elezioni negli Stati membri,

44 Cfr. www.e-voting.at

45 Elezione del Parlamento nel giugno 2002 a Vandoeuvre-lès-Nancy e referendum internet a Issy-les-Moulineaux nel novembre 2002.

46 P. es. da ultimo nell'ambito di elezioni amministrative del 17 novembre 2002 a Cremona.

47 Da ultimo in concomitanza con l'elezione del Parlamento del 14 marzo 2004 a Lugo (Mosteiro-Pol), Zamora e Toro (Zamora).

48 P. es. www.i-vote.de e <http://forschungsprojekt-wien.de>

49 Cfr. http://europa.eu.int/information_society/eeurope

50 Cfr. Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche.

51 Ad es. in Austria: Signaturgesetz (legge sulle firme elettroniche), BGBl. I Nr. 190/1999 idgF (modificata l'ultima volta da BGBl. I Nr. 152/2001) e Signaturverordnung (ordinanza sulle firme elettroniche), BGBl. II Nr. 30/2000.

52 Cfr. Jefferson D., Rubin A.D., Simons B., Wagner D., A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), 2004, www.servesecurityreport.org e McGaley M., Gibson J.P., Electronic Voting, A Safety Critical System, Department of Computer Science, National University of Ireland, Maynooth 2003, www.cs.may.ie/research/reports/2003/nuim-cs-tr-2003-02.pdf.

la raccomandazione definisce solo standard minimi. Secondo la raccomandazione, il voto elettronico deve rispettare tutti i principi delle votazioni ed elezioni democratiche ed essere affidabile e sicuro quanto votazioni ed elezioni non elettroniche; sono considerati particolarmente importanti un elevato livello di sicurezza del voto elettronico, la specificazione del voto elettronico quale ulteriore variante del voto e la neutralità tecnologica (accesso multicanale)⁵³. La Commissione europea per la democrazia attraverso il diritto («Commissione di Venezia»), un organo consultivo del Consiglio d'Europa, ha esaminato nel suo «Codice di buona condotta elettorale» il voto elettronico dal punto di vista della tutela dei diritti democratici fondamentali. Secondo il parere della Commissione, il voto elettronico può essere autorizzato solo se realizzato in modo sicuro e affidabile; in particolare il votante deve avere una conferma del voto e, se lo esige il diritto nazionale, deve potervi apportare una correzione. In questo contesto, deve essere garantita la trasparenza del sistema⁵⁴.

Nei mesi di luglio 2004 e aprile 2005, l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) ha organizzato a Vienna due ulteriori incontri sullo svolgimento e sull'osservazione di elezioni. Molti Stati partecipanti dell'OSCE vorrebbero introdurre il voto elettronico. L'OSCE ritiene indispensabile tenere maggiormente conto di questo nuovo sviluppo nell'ambito degli impegni elettorali e delle missioni di osservazione elettorale. Inoltre in futuro l'OSCE desidera ricorrere, nelle missioni di osservazione elettorale, a esperti che aiutano a valutare l'attuazione degli impegni nel contesto tecnico⁵⁵. In occasione delle presidenziali americane di novembre 2004, ad esempio, le macchine di voto impiegate nei seggi elettorali di molti Stati federali sono state sottoposte a controlli a campione per quanto riguarda eventuali difetti⁵⁶.

4.5 Conclusioni

Prima di poter impiegare il loro sistema di voto elettronico, i Cantoni pilota di Ginevra, Neuchâtel e Zurigo avevano dovuto realizzare una vasta serie di test seguiti da esperti esterni. In questo contesto dovevano essere sperimentate sia le misure adottate per la sicurezza tecnica sia le concomitanti misure organizzative che si avvalgono della collaborazione tra Comuni, Cantone, Confederazione, popolazione avente diritto di voto e pubblico.

⁵³ Cfr. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting, adottata dal Comitato dei ministri il 30 settembre 2004 in occasione della 898ª riunione.

⁵⁴ Code de bonne conduite en matière électorale (Codice di buona condotta elettorale) adottato dalla Commissione europea per la democrazia attraverso il diritto, luglio/ottobre 2002, n. 3.2 cpv. IV del Codice come pure n. 3.2.2.3 del corrispondente rapporto esplicativo, cfr. avviso n. 190/2002 della Commissione di Venezia del 9 ottobre 2002, [www.venice.coe.int/docs/2002/CDL-EL\(2002\)005-f.asp](http://www.venice.coe.int/docs/2002/CDL-EL(2002)005-f.asp) o la traduzione in tedesco [www.venice.coe.int/docs/2002/CDL-AD\(2002\)023-ger.pdf](http://www.venice.coe.int/docs/2002/CDL-AD(2002)023-ger.pdf).

⁵⁵ OSCE/ODIHR, Supplementary Human Dimension Meeting on Electoral Standards and Commitments, Vienna, 15/16 luglio 2004; Supplementary Human Dimension Meeting on Challenges of Election Technologies and Procedures, Vienna, 21/22 aprile 2005 (cfr. www.osce.org/item/9742.html).

⁵⁶ Cfr. per la missione di osservazione elettorale OSCE 2004 negli USA, il Final Report on the 2 November 2004 Elections in the United States of America, marzo 2005, www.osce.org/item/13658.html e per le direttive dell'OSCE in materia di verifica delle procedure elettorali elettroniche, l'Election Observation Handbook, quinta edizione, aprile 2005, pag. 44, www.osce.org/item/14004.html?ch=240.

Dopo la prima prova pilota effettuata a Anières (GE) il 19 gennaio 2003 e ulteriori prove comunali o cantonali molto limitate, i sistemi sviluppati nei tre Cantoni sono stati impiegati sino alla fine del 2005 complessivamente cinque volte con successo e senza disturbi nell'ambito di votazioni popolari federali. Queste prove sono servite alla verifica complementare e in campo della fattibilità in condizioni reali.

Tabella 1

Prove pilota eseguite in occasione di votazioni popolari federali

| Votazione popolare federale del: | Impiego del voto elettronico nel: | Estensione della prova pilota: | Quantità di voti elettronici (in percento dei voti) |
|----------------------------------|--|--|---|
| 26 settembre 2004 | Cantone di Ginevra: Comuni di Anières, Carouge, Coligny, Meyrin | 22 137 aventi diritto di voto | 2723 voti (21,8 %) |
| 28 novembre 2004 | Cantone di Ginevra: Comuni di Anières, Carouge, Coligny, Collonge-Bellerive, Meyrin, Onex, Vandoeuvres, Versoix | 41 431 aventi diritto di voto | 3755 voti (22,4 %) |
| 25 settembre 2005 | Cantone di Neuchâtel | 1732 utilizzatori del Guichet Unique con diritto di voto | 1178 voti (68,0 %) |
| 27 novembre 2005 | Cantone di Zurigo: Comuni di Bertschikon, Bülach, Schlieren | 16 726 aventi diritto di voto | 1154 voti (243 per SMS) (22,1 %) |
| 27 novembre 2005 | Cantone di Neuchâtel | 2469 utilizzatori del Guichet Unique con diritto di voto | 1345 voti (55,1 %) |

In media oltre il 22 per cento degli elettori che hanno votato nell'ambito delle prove pilota ha scelto il voto elettronico. Nel Cantone di Neuchâtel è stata registrata una percentuale largamente superiore (55–68 %) dato il grande interesse mostrato dalla cerchia di utenti del Guichet Unique.

Le prove pilota giuridicamente valide realizzate in Svizzera hanno attirato anche l'interesse di organismi internazionali. Il Consiglio d'Europa, ad esempio, quale prima organizzazione internazionale, ha adottato il 30 settembre 2004, con riferimento all'ordinanza sui diritti politici (ODP, in particolare gli articoli 27a–27q), una raccomandazione contenente i principi di base per l'impiego di mezzi elettronici nell'ambito di votazioni⁵⁷. La Svizzera ha potuto far confluire le proprie esperienze anche nell'OSCE in occasione delle discussioni su obblighi complementari dei Paesi partecipanti nell'ambito di votazioni ed elezioni democratiche⁵⁸.

⁵⁷ Recommendation Rec(2004)11 du Comité des Ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (Raccomandazione R (2004) 11 del Comitato dei ministri agli Stati membri sulle norme giuridiche, tecniche e organizzative del voto elettronico).

⁵⁸ Cfr. n. 4.4.1

5 Valutazione delle prove pilota

Nel seguito i progetti pilota sono valutati in base ai criteri introdotti nel numero 3. Quindi viene mostrato come potrebbe essere attuata l'introduzione del voto elettronico in Svizzera (n. 5.4).

5.1 Utilità e ripercussioni sulla democrazia diretta

La Svizzera fa parte dei Paesi più progrediti per quanto riguarda l'accesso a Internet. Come risulta dall'ultima indagine della società di ricerche e studi dei media pubblicitari WEMF/REMP, quasi quattro milioni di cittadini svizzeri, di cui il 43 per cento donne, dispongono oggi a casa di un collegamento Internet. L'indagine è stata condotta tra aprile e settembre 2004 presso 11 000 persone domiciliate in Svizzera⁵⁹. L'81,7 per cento degli utenti di Internet in Svizzera impiega la posta elettronica; il 67 per cento ricorre ai servizi dei motori di ricerca; il 40 per cento afferma di leggere regolarmente notizie e informazioni («news») in Internet; il 18,7 per cento consulta articoli di giornali e riviste e il 15 per cento degli utenti di Internet si procura informazioni sugli orari. Poco apprezzato lo shopping on line, praticato solo dal 4,3 per cento degli utenti. Il 4,7 per cento partecipa alle aste on line e il 12,3 per cento usa l'e-banking. Considerate queste cifre, appare logico impiegare l'Internet anche per la partecipazione democratica diretta.

Il voto elettronico potrebbe contribuire a far aumentare la partecipazione al voto? Secondo il professore zurighese di scienze politiche Hanspeter Kriesi, il voto elettronico permette di mobilitare lo strato della popolazione che si astiene particolarmente spesso dal votare, cioè i giovani. Due studi che sono serviti da base al nostro Rapporto del 9 gennaio 2002 sul voto elettronico (FF 2002 567–621, segnatamente: 575 seg. e allegati) sono giunti a risultati differenti per quanto riguarda l'ipotesi di un aumento della partecipazione al voto da parte del voto elettronico. Il centro di studio e documentazione sulla democrazia diretta di Ginevra (Centre d'études et de documentation sur la démocratie directe) (c2d) ha stimato al massimo al 9 per cento il potenziale di aumento della partecipazione al voto per il Cantone di Ginevra. Il professor Wolf Linder dell'Università di Berna ha previsto un aumento massimo di 1,7 punti percentuali della partecipazione a livello nazionale.

Il voto elettronico potrebbe però anche portare a cambiamenti indesiderati: secondo il parere di alcuni esperti, nasconde il rischio di una «deritualizzazione» delle procedure di voto. Per Yannis Papadopoulos, professore all'Università di Losanna, il voto elettronico rappresenta un ulteriore passo verso la privatizzazione della votazione e dell'elezione politica. Quanto più la partecipazione politica viene privatizzata tanto meno gli aventi diritto di voto si interessano dell'opinione degli altri. Non è stato possibile esaminare questa problematica nell'ambito delle prove pilota regionali e di durata limitata. Tuttavia la maggioranza degli esperti presenti a un convegno scientifico dell'Associazione svizzera per l'informatica giuridica ha giudicato inevitabile, anche se non privo di rischi, lo sviluppo del voto elettronico per il mantenimento della democrazia diretta in Svizzera. Ritirarsi nella sfera privata è una tendenza che

⁵⁹ WEMF AG für Werbemedienforschung (Società di ricerche e studi dei media pubblicitari), WEMF-Report Plus, aprile 2005; www.wemf.ch/pdf/d/Report_Plus_1_05_d.pdf.

si riscontra dappertutto nella società; il voto per corrispondenza o per via elettronica non è però la causa, ma la conseguenza di questa tendenza⁶⁰.

Su incarico del Parlamento, la Cancelleria federale provvede affinché le prove pilota in materia di voto elettronico siano sorrette da una consulenza scientifica; in particolare, conformemente all'articolo 8a capoverso 3 LDP, sono rilevati statisticamente dati concernenti sesso, età e formazione di coloro che utilizzano potenzialmente ed effettivamente il voto elettronico per votare.

5.1.1 Studio sul potenziale 2003–2004

Nello studio del 18 gennaio 2005 commissionato dalla Cancelleria federale «Il potenziale del voto elettronico»⁶¹ dell'Istituto di ricerca gfs.bern è stata esaminata empiricamente la questione della desiderabilità (potenzialità⁶²) del voto elettronico presso la popolazione svizzera avente diritto di voto.

⁶⁰ Cfr. Muralt Müller, Hanna e Koller Thomas (Hrsg.), E-Voting, Tagung 2002 für Informatikrecht, Berna 2002. Sul segreto del voto in generale e nell'ambito del voto elettronico cfr. anche Braun, Diss. 2005.

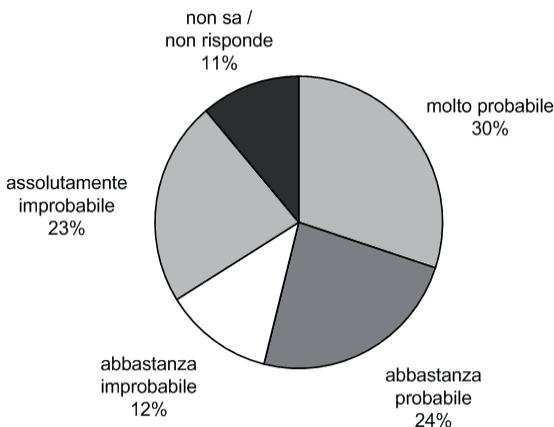
⁶¹ Istituto di ricerche gfs.bern: Das Potenzial der elektronischen Stimmabgabe (Il potenziale del voto elettronico), studio realizzato su incarico della Cancelleria federale, Berna 2005, cfr. la documentazione complementare 11a. L'inchiesta sul potenziale del voto elettronico si basa su quattro analisi VOX (analisi post-voto di votazioni popolari federali) degli anni 2003 e 2004. Sono stati intervistati 4018 cittadini svizzeri aventi diritto di voto a livello federale.

⁶² Potenzialità sono predisposizioni o disponibilità ad agire. A seconda della forma esprimono solo la rappresentazione di un'azione, il desiderio di un'azione o l'intenzione reale di un'azione. Ma non sono azioni: queste hanno luogo solo con parti del potenziale.

Il potenziale del voto elettronico presso la popolazione svizzera avente diritto di voto

«Se avesse la possibilità di votare elettronicamente è molto probabile, abbastanza probabile, abbastanza improbabile o assolutamente improbabile per Lei utilizzare questa modalità di voto?»

In per cento degli aventi diritto di voto



© gfs.bern, voto elettronico, 2003/2004 (N=4018)

Due su tre aventi diritto di voto dispongono dell'accesso a Internet. La diffusione presso gli aventi diritto di voto giovani che hanno una formazione superiore è ancora più grande. Secondo l'indagine, il 54 per cento degli intervistati può immaginarsi di esprimere il voto via Internet. Il potenziale del voto elettronico è pertanto a disposizione di più della metà degli aventi diritto di voto in Svizzera. Per oltre un terzo di loro tuttavia è abbastanza o assolutamente improbabile impiegare il voto elettronico.

Sono particolarmente spesso ragioni di usabilità che spingono i potenziali utilizzatori a impiegare il voto elettronico (considerato «più comodo/più semplice/non complicato»); sono invece le paure per quanto riguarda la sicurezza dei dati le ragioni per cui le persone con ogni probabilità non lo utilizzerebbero. La maggior parte degli intervistati ritiene il voto per corrispondenza più sicuro di quello elettronico.

Non è sorprendente che siano soprattutto le persone che accedono quotidianamente a Internet e che lo utilizzano anche regolarmente per attività professionali o private a impiegare in misura rilevante il voto elettronico.

Per quanto riguarda l'entità del potenziale sono fattori determinanti le seguenti variabili: la professione, l'età, la formazione, il sesso, il reddito e il genere di insediamento. Secondo l'istituto gfs.bern ciò prova che il voto elettronico è un medium molto giovane. In genere, i nuovi media non si diffondono in modo neutrale dal punto di vista sociologico e socioeconomico. Il voto elettronico è destinato prevalentemente a uno strato alto della popolazione, di età giovane, di sesso maschile, che vive in insediamenti urbani. Tuttavia il potenziale è superiore al 50 per cento anche presso le persone di età tra i 40 e i 65 anni e presso le persone di uno strato sociale

medio. Nella Svizzera romanda il potenziale è generalmente superiore rispetto alle altre regioni linguistiche del Paese.

Degno di rilievo è anche il fatto che il voto elettronico è particolarmente apprezzato dalle persone che non partecipano mai o solo sporadicamente a votazioni e elezioni. Ciò parlerebbe in favore non solo della sostituzione di altre forme di votazione, ma anche della probabilità di un aumento della partecipazione al voto.

L'entità del potenziale varia poi anche con il variare del coinvolgimento politico dei votanti. Se aumentano l'interesse per le questioni politiche e la partecipazione a discussioni politiche aumenta anche il potenziale del voto elettronico. Per quanto riguarda l'appartenenza politica dei votanti si sono potute determinare solo ripercussioni di lieve entità sul potenziale del voto elettronico. Le differenze tra i simpatizzanti dei diversi partiti rientrano tutte nei margini dell'errore di campionamento. Il voto elettronico deve essere considerato una grandezza neutrale per quanto riguarda le sue potenziali ripercussioni sul rapporto di forze tra i partiti politici.

Secondo l'istituto gfs.bern non si può escludere che il voto elettronico abbia un influsso sulla mobilitazione. Impiegare il voto elettronico è molto probabile per il 30 per cento degli aventi diritto di voto e abbastanza probabile per un ulteriore 24 per cento. Non si tratta in primo luogo di aventi diritto di voto che partecipano anche effettivamente, ma di aventi diritto di voto che decidono di volta in volta se vogliono partecipare. Se il voto elettronico è configurato secondo i principi dell'usabilità, si può partire dal presupposto che la partecipazione al voto aumenti relativamente. I fattori che influiscono principalmente sulla mobilitazione non sono legati direttamente alle possibilità di votare. Si assisterà dunque soprattutto a una sostituzione a scapito del voto per corrispondenza. Un'eventuale mobilitazione superiore concerne in primo luogo giovani che in genere sono ampiamente sottorappresentati e apprezzano molto il voto elettronico. Il secondo gruppo che potrebbe partecipare maggiormente con il voto elettronico è quello degli Svizzeri all'estero⁶³.

5.1.2 Sondaggi nell'ambito delle prove pilota cantonali in occasione di votazioni popolari federali

5.1.2.1 Cantone di Ginevra⁶⁴

In occasione degli scrutini di Carouge e Meyrin, nella primavera 2004, e del primo scrutinio federale svolto via Internet, nel settembre 2004, il Cantone di Ginevra ha incaricato il centro di studio e di documentazione sulla democrazia diretta dell'Università di Ginevra (c2d) di tracciare il profilo e le motivazioni degli utilizzatori del voto on line e di specificare che cosa li distingue dagli altri elettori. Questi studi hanno evidenziato due aspetti essenziali.

⁶³ Istituto di ricerche gfs.bern: Internationale SchweizerInnen (Svizzeri all'estero internazionali), rapporto finale sul primo sondaggio rappresentativo on line condotto tra gli Svizzeri all'estero aventi diritto di voto per l'OSE e swissinfo/SRI. Berna 2003, www.gfs.ch/auslandschweizer.html.

⁶⁴ Centre d'études et de documentation sur la démocratie directe de l'Université de Genève, Analyse du scrutin du 26 septembre 2004 dans quatre communes genevoises (Anières, Carouge, Cologny e Meyrin), luglio 2005, cfr. la documentazione complementare 11b.

I fattori determinanti per scegliere di utilizzare il voto on line invece del voto per corrispondenza e del voto all'urna non sono l'età, il reddito, il livello di formazione o il posizionamento politico, ma variabili «informatiche» come la fiducia nelle comunicazioni in Internet e le conoscenze informatiche. Quest'ultima variabile non significa che si debba essere specialisti di computer per votare on line, ma semplicemente avere familiarità con il PC. Il livello di conoscenza non risulta effettivamente da una valutazione oggettiva, ma da un'autovalutazione soggettiva delle persone intervistate. Le tre modalità di scrutinio, voto all'urna, voto per corrispondenza e voto via Internet, sono politicamente neutrali. In altre parole, è impossibile indovinare le preferenze politiche di un elettore sulla base della modalità di voto da lui scelta.

Secondo queste due osservazioni fondamentali, il ricorso al voto on line risulta da una scelta personale e indica un modo di vita di cui le tecnologie dell'informazione costituiscono un asse portante. In nessun caso è un indicatore che permette a priori di differenziare gli individui in utilizzatori e non-utilizzatori sulla base di caratteristiche che indicano appartenenza a un «rango» sociale.

Questa constatazione rimette in discussione certe spiegazioni semplici per non dire semplicistiche che si trovano nella letteratura del ramo e nella stampa. Anche se sappiamo, ad esempio, che le donne votano meno tramite Internet degli uomini e che i giovani apprezzano molto questo strumento di voto, lo studio mostra che queste variabili non sono in realtà di grande aiuto per spiegare la scelta o meno del voto elettronico.

Inoltre, i controlli effettuati dalle autorità ginevrine hanno evidenziato che la distribuzione temporale dei voti non è la stessa per il voto per corrispondenza e per quello elettronico. I voti per corrispondenza seguono un andamento irregolare nel corso delle quattro settimane che dura uno scrutinio: nella terzultima e nell'ultima settimana prima della votazione raggiungono rispettivamente il 40 e il 30 per cento; i voti elettronici si concentrano invece nella misura di oltre il 50 per cento sull'ultima settimana e addirittura di quasi il 30 per cento sulle ultime 36 ore di apertura dello scrutinio.

Si dovrebbe disporre di una serie di risultati molto più consistente per poter procedere a uno studio dell'impatto del voto elettronico sulla partecipazione. Si possono tuttavia osservare le due tendenze seguenti:

- Internet «toglie» elettori al voto per corrispondenza, ma non al voto all'urna, la cui frequenza è rimasta nella media (5 %);
- la classe di età dei 18–29 anni, che rappresenta il 10 per cento dell'elettorato, non costituisce che il 7 – 8 per cento dei votanti effettivi senza il voto on line. Se viene offerto il voto via Internet, il peso di questa classe di età nel gruppo dei votanti sale al suo peso demografico, cioè al 10 per cento.

Pertanto la generalizzazione del voto elettronico potrebbe non solo far aumentare la partecipazione, ma anche migliorare la rappresentatività della scelta degli elettori con l'inclusione di un più grande numero di giovani nel numero dei votanti.

Negli otto scrutini per i quali nel Cantone di Ginevra è stata offerta la modalità di voto Internet, ossia per 26 domande agli elettori, i risultati del voto elettronico hanno sempre rispecchiato quelli della maggioranza finale.

5.1.2.2

Cantone di Neuchâtel

Il Cantone di Neuchâtel ha organizzato per la prima volta un voto elettronico in occasione della votazione federale del 25 settembre 2005. Per conoscere meglio le opinioni degli elettori, il Cantone di Neuchâtel ha svolto un'indagine⁶⁵ sulla soddisfazione delle persone che disponevano della possibilità di votare via Internet. Tutte le persone interessate hanno ricevuto una e-mail con le informazioni utili per partecipare all'indagine svolta dal 29 settembre al 21 ottobre 2005. Resta da sottolineare il grande interesse mostrato per il progetto: più del 58 per cento delle persone ha risposto alle domande.

Spesso considerato come uno strumento per i giovani, si constata invece che anche gli «anziani» mostrano interesse per il nuovo mezzo di comunicazione Internet. Con il 16,5 per cento di oltre 60 anni e quasi il 27 per cento tra i 50 e i 59 anni, questo segmento è ben rappresentato tra gli utilizzatori del Guichet Unique.

Per quanto riguarda la domanda relativa all'accesso internet, due terzi degli utilizzatori dispongono di un accesso a casa e sul posto di lavoro e il restante terzo dispone di un accesso unicamente a casa. Pochissimi gli utilizzatori che hanno un accesso solo sul posto di lavoro.

I risultati sull'impiego di Internet, sulle conoscenze informatiche e sulla sicurezza dei dispositivi di immissione denotano il grande interesse per l'impiego delle nuove tecnologie della comunicazione.

Le risposte sulle abitudini di voto non devono essere considerate sorprendenti visto che provengono soprattutto da elettori che partecipano regolarmente ai differenti scrutini utilizzando il voto per corrispondenza, come più del 96 per cento dei votanti.

I motivi per cui certi utilizzatori non hanno potuto impiegare il voto elettronico sono principalmente problemi tecnici di configurazione del posto di lavoro. Il 6,9 per cento (il 5,8 % per un problema di accesso al Guichet Unique e l'1,1 % per un guasto del computer) non corrisponde al numero di problemi registrato presso il supporto tecnico del Cantone di Neuchâtel. Molti utilizzatori non hanno mai contattato il servizio di supporto. È dunque indispensabile attirare l'attenzione di coloro che hanno problemi che possono prendere contatto per e-mail con il supporto tecnico del Cantone.

Gli aspetti dell'usabilità e della fiducia nei confronti del voto elettronico hanno fatto registrare risultati molto buoni. Con oltre l'87 per cento di persone soddisfatte dal punto di vista dell'usabilità e oltre il 94 per cento da quello della fiducia, si possono considerare raggiunti i primi obiettivi. Alcune osservazioni e proposte dovranno essere analizzate nelle prossime tappe. Sono interessati essenzialmente aspetti del confort come la registrazione del codice di validazione.

Diversamente dai vantaggi del voto elettronico, che concernono più aspetti, gli inconvenienti si concentrano prevalentemente sulla questione del divario digitale. Anche se non è messa in discussione la soppressione delle due altre modalità di voto, si constata che questo elemento resta la preoccupazione principale nonostante il fatto che il numero di internauti non smetta di aumentare.

⁶⁵ Cantone di Neuchâtel, Enquête de satisfaction, scrutin du 25 septembre 2005, novembre 2005, cfr. la documentazione complementare 11c.

Il fatto che il voto elettronico sia approvato da quasi il 99 per cento degli utilizzatori dimostra in maniera molto chiara la volontà di un cambiamento nei processi di lavoro con le amministrazioni pubbliche.

Dall'ultima domanda, che concerneva l'aumento della partecipazione agli scrutini, non è emersa una tendenza reale dato che la maggior parte delle persone erano elettori con l'abitudine di votare regolarmente.

5.1.2.3 Cantone di Zurigo

Nel Cantone di Zurigo è stato svolto, nell'ambito della prova pilota in occasione della votazione popolare federale del 27 novembre 2005, un sondaggio⁶⁶ presso gli aventi diritto di voto dei Comuni di Bertschikon, Bülach e Schlieren. Complessivamente sono state intervistate per telefono 600 persone. Nei tre Comuni pilota hanno utilizzato particolarmente spesso il voto elettronico persone di età da giovane a media e di sesso maschile. In una percentuale superiore alla media, gli utilizzatori svolgono un'attività lavorativa e hanno seguito una formazione professionale postuniversitaria. Chi vota in modo selettivo è più aperto nei confronti del voto elettronico di coloro che votano regolarmente. Hanno scelto prevalentemente la via elettronica le persone che hanno un reddito alto, grande fiducia in Internet e che utilizzano le nuove tecnologie con competenza e frequenza.

Dato che il sondaggio era limitato regionalmente ai Comuni pilota è difficile rispondere alla domanda se il voto elettronico può aumentare la partecipazione al voto nel Cantone di Zurigo. Sia persone che votano in modo tradizionale che persone che votano per corrispondenza sono pronte a passare alle possibilità di votare elettronicamente. La maggior parte dei votanti è rimasta fedele alla propria modalità di voto. Vi è però sia tra le persone che votano recandosi all'urna che tra quelle che votano per corrispondenza un gran numero di votanti che ha optato per la variante elettronica. Il 5 per cento di chi si è servito del voto elettronico ha dichiarato che non avrebbe partecipato alla votazione senza la possibilità elettronica. Questi risultati lasciano presumere che il voto elettronico potrebbe indurre alcuni non votanti a votare e alcune persone che votano saltuariamente a votare più spesso.

Dal sondaggio risulta infine che l'opinione di chi vota con voto elettronico può, a seconda del testo, differire da quella degli altri elettori. Tuttavia, il voto elettronico non modifica il rapporto di forze tra partiti politici. A questa conclusione giungono tutti i sondaggi condotti nell'ambito dei progetti pilota.

5.1.2.4 Inchieste di terzi

Accanto alle inchieste avviate direttamente, nell'ambito dei progetti pilota, dalla Cancelleria federale o dai Cantoni pilota, anche terzi hanno voluto conoscere a più riprese l'opinione dei cittadini sul voto elettronico. Da un sondaggio effettuato nell'ottobre 2005 su incarico del giornale Cooperazione dall'istituto demoscopico

⁶⁶ Centre d'études et de documentation sur la démocratie directe de l'Université de Genève, Umfrage bei Stimmberechtigten der Zürcher Gemeinden Bertschikon, Bülach und Schlieren anlässlich des Pilotversuchs vom 27. November 2005, Ginevra, Firenze, marzo 2006, cfr. la documentazione complementare 11d.

Link presso 681 persone nella Svizzera tedesca e nella Svizzera romanda risulta, ad esempio, che il 57 per cento degli Svizzeri è favorevole al voto elettronico per SMS. Il 25 per cento di loro apprezza molto questa nuova variante di voto. L'altro 32 per cento dei fautori sarebbe propenso a servirsi della nuova tecnologia per votare. Il 23 per cento si è espresso, invece, prevalentemente contro e il 17 per cento degli intervistati non impiegherebbe il voto elettronico tramite SMS. Il 3 per cento non si è espresso⁶⁷.

Secondo il terzo barometro di tendenza sul governo elettronico della scuola universitaria professionale di Berna del marzo 2006 ben il 70 per cento della popolazione svizzera utilizzerebbe il voto elettronico se potesse. Lo studio afferma che il voto elettronico è al terzo posto nella lista dei desiderata dei cittadini dopo la notifica e il ritiro per via elettronica in caso di cambiamento di domicilio e dopo la notifica e il ritiro per via elettronica di licenze di condurre e di veicoli⁶⁸.

5.1.3 Le facilitazioni portano una maggiore partecipazione al voto?

Per rispondere alla domanda si possono utilizzare, oltre ai sondaggi sul potenziale del voto elettronico effettuati nell'ambito dei progetti pilota cantonali, le esperienze fatte con il voto per corrispondenza, che viene già impiegato da diverso tempo.

Il voto elettronico e quello per corrispondenza hanno in comune che sono entrambi voti a distanza. Gli elettori non devono recarsi presso un seggio elettorale per esprimere il voto. La scheda può essere compilata a casa, alla scrivania o al PC, ed essere spedita per posta o per via elettronica. I vantaggi di questa facilitazione sono evidenti: gli elettori possono esprimere il voto indipendentemente dal tempo e dal luogo.

Rispetto all'estero, la Svizzera ha liberalizzato il voto prima e in misura più ampia⁶⁹. La liberalizzazione ha portato, oltre al voto generale per corrispondenza introdotto in tutta la Svizzera nel 1994, già prima notevoli semplificazioni. Il diritto di voto ad esempio può essere esercitato in molti Cantoni anche anticipatamente di persona o per procura.

Queste facilitazioni, ma in particolare il voto a distanza, corrispondono alle esigenze di una società moderna e mobile. Secondo le previsioni, il voto per corrispondenza ha riscosso notevole successo presso gli aventi diritto di voto in Svizzera dopo la sua introduzione generale nel 1994⁷⁰.

Sino alla fine della seconda guerra mondiale, è stata registrata nella media decennale una partecipazione al voto costantemente superiore al 50 per cento della popolazione avente diritto di voto. Negli anni Sessanta e fino agli Ottanta, la partecipazione al voto è quindi scesa parzialmente sotto il 40 per cento. Tra il 1995 e il 2005 è leggermente salita e ha registrato valori medi del 44,5 per cento. In alcuni Cantoni della Svizzera romanda, nei Cantoni di Basilea Città e di Nidwaldo questo aumento coincide temporalmente con l'introduzione cantonale del voto facilitato per corrispon-

⁶⁷ Giornale Coopzeitung n. 42 del 19 ottobre 2005, pag. 3.

⁶⁸ Berner Fachhochschule, 3. E-Government Trendbarometer, Nutzen und Trends aus Bürgersicht, Berna, marzo 2006, www.wirtschaft.bfh.ch/index.php?nav=375.

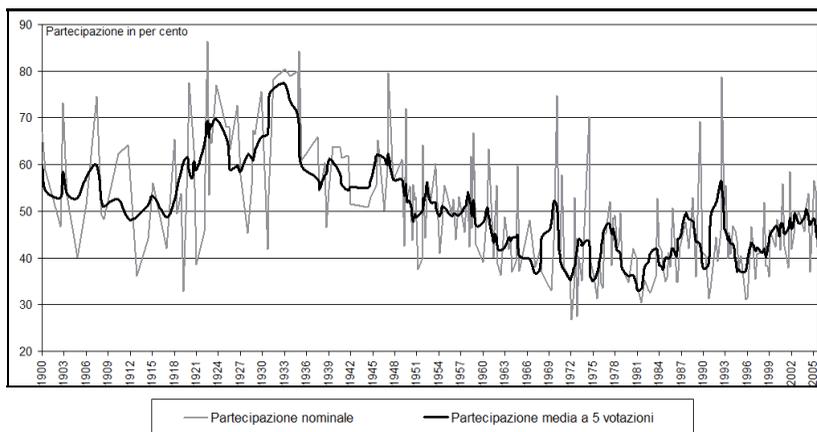
⁶⁹ Cfr. Braun Diss. 2005, n. marg. 176 segg., 189, 199 segg., 415 segg., 429 segg., 512 segg.

⁷⁰ Art. 5 cpv. 3 LDP, cfr. RU 1994 2414; FF 1993 III 309

denza⁷¹. Nello stesso periodo di tempo, all'estero si è registrata una costante riduzione della partecipazione al voto.

Figura 2

La partecipazione al voto nelle votazioni popolari dal 1900



La Cancelleria federale ha condotto nel 2005 presso i Cantoni e i Comuni due sondaggi⁷² complementari sul voto per corrispondenza. Nell'ambito del primo sondaggio effettuato in occasione della votazione popolare federale del 5 giugno 2005 i Cantoni cittadini di Basilea Città e Ginevra, ma anche i Cantoni di Lucerna, Vaud, Neuchâtel, Obvaldo e San Gallo hanno registrato una percentuale di voti per corrispondenza superiore al 90 per cento. In due Cantoni invece la percentuale dei voti per corrispondenza è risultata largamente al di sotto della media: nel Cantone di Glarona con il 17 per cento e in quello di Sciaffusa con il 25 per cento dei voti. Nel Cantone del Vallese la quota, che nel 2004 ammontava a un marginale 5 per cento, è salita, nel 2005, al 67 per cento con il passaggio al voto incondizionato per corrispondenza⁷³.

D'intesa con la Conferenza Svizzera dei cancellieri di Stato, la Cancelleria federale ha svolto, in occasione della votazione popolare del 27 novembre 2005, una rilevazione supplementare presso tutti i Comuni svizzeri sulla percentuale dei voti ricevuti per corrispondenza. L'81,5 per cento dei voti è stato espresso per corrispondenza: nei Cantoni SZ, OW, NW, ZG e SG, più del 90 per cento, nei Cantoni LU, BS, VD, NE e GE addirittura più del 95 per cento. In otto Cantoni (GL, SH, AR, AI, TG, TI, VS e JU) invece la percentuale dei voti alle urne è stata superiore al 30 per cento. La partecipazione più bassa al voto per corrispondenza è stata registrata nei Cantoni GL

⁷¹ Cfr. per i risultati di tutte le votazioni popolari dal 1848: www.bk.admin.ch/ch/d/pore/va/index.html.

⁷² Cfr. la documentazione complementare 8.

⁷³ L'unico Cantone che continua a vincolare il voto per corrispondenza a determinate condizioni per le votazioni ed elezioni cantonali e comunali è il Cantone Ticino. Cfr. art. 32 della legge del 7 ottobre 1998 sull'esercizio dei diritti politici.

e SH⁷⁴. La maggior parte dei voti per corrispondenza è spedita nel corso delle ultime due settimane che precedono la domenica della votazione. Fanno eccezione i Cantoni NE e GE: oltre un terzo degli elettori spedisce i voti per corrispondenza già nella terzultima settimana prima del giorno della votazione. Dal punto di vista delle scadenze, per questi due Cantoni, le campagne precedenti le votazioni devono pertanto essere coordinate diversamente da quelle nelle altre regioni della Svizzera. Nel Cantone GE, la percentuale dei voti per corrispondenza ricevuti registra un'ulteriore impennata durante l'ultima settimana. Le prove pilota del voto elettronico nei Cantoni GE, NE e ZH hanno mostrato che tendenzialmente i voti elettronici aumentano costantemente dalla terzultima all'ultima settimana prima della data della votazione. Molti decidono solo nel corso delle ultime ore prima della chiusura delle urne di votare per via elettronica. Sullo svolgimento delle campagne da parte dei partiti e delle associazioni, il voto elettronico non ha praticamente nessun effetto distorsivo⁷⁵.

Nel 2002 eravamo scettici nei confronti della valutazione positiva di alcuni esperti su un eventuale aumento della partecipazione al voto dovuto al voto elettronico⁷⁶. Questo atteggiamento scettico deve essere mantenuto anche dopo lo svolgimento e il monitoraggio scientifico di progetti pilota. Il potenziale inaspettatamente alto del voto elettronico registrato nelle inchieste riassunte nel numero 5.1 nonché gli indizi di un possibile aumento della partecipazione al voto in tutti e tre i Cantoni devono prima essere confermati in diverse prove capillari a livello cantonale.

5.1.4 Conclusione

I risultati delle precedenti analisi sociodemografiche rispecchiano i risultati dei sondaggi svolti da terzi sotto molti punti di vista:

- il voto elettronico è accettato dalla maggioranza degli Svizzeri aventi diritto di voto;
- un terzo circa degli intervistati afferma di voler impiegare il voto elettronico se viene introdotto;
- un quarto fino a un quinto degli intervistati non può immaginarsi di impiegare il voto elettronico o non ne approverebbe l'introduzione.

La domanda relativa a un eventuale aumento della partecipazione al voto non può essere chiarita in modo definitivo sotto l'aspetto scientifico neanche dopo il monitoraggio scientifico di varie prove pilota. La valutazione di questa domanda dipende dall'entità del potenziale del voto elettronico presso le persone che non partecipano mai o solo sporadicamente alle votazioni popolari⁷⁷.

⁷⁴ GL e AI sono rimasti gli unici Cantoni Svizzeri con Landsgemeinde. Il Cantone SH è l'unico in cui vige ancora l'obbligo del voto.

⁷⁵ Cfr. per i risultati dettagliati del sondaggio, la documentazione complementare 8, n. 5 e 6.
⁷⁶ FF 2002 576 seg.

⁷⁷ Per altre osservazioni su un ulteriore aumento della partecipazione dovuto al voto elettronico, cfr. n. 5.1.3.

La liberalizzazione del voto può essere considerata quasi un obbligo per la moderna società mobile. Le abitudini di vita richiedono, prima o poi, la diversificazione delle possibilità di voto, la quale, tuttavia, può anche aumentare il rischio che i processi decisionali democratici siano soggetti a guasti.

5.2 Rischi e misure di sicurezza

5.2.1 L'architettura di sicurezza dei sistemi cantonali⁷⁸

Nell'ambito del voto elettronico si distinguono le zone «ambiente dell'utente», «rete dell'amministrazione» e «zona di alta sicurezza».

Sono considerati «ambiente dell'utente» gli apparecchi di immissione che i votanti utilizzano per esprimere il voto elettronico cioè PC, PC portatile (laptop), telefoni cellulari o PDA⁷⁹. Diversi provider e fornitori di telefonia mobile assicurano la comunicazione di questi mezzi di immissione con l'applicazione di voto. Gli apparecchi di immissione hanno configurazioni molto diverse (sistema operativo, genere di browser), al di fuori dell'ambito di influenza dell'applicazione di voto. La responsabilità della sicurezza del mezzo di immissione utilizzato deve essere pertanto assunta esclusivamente dall'utente o dal gestore responsabile (protezione antivirus, firewall ecc.).

Una seconda zona può essere specificata con il termine di «rete dell'amministrazione». Questa zona è contraddistinta da possibilità di accesso limitate e dalla separazione da Internet. Le reti dell'amministrazione ad accesso limitato svolgono tutte le transazioni dell'amministrazione di voto elettronico con i Comuni, ad esempio lo scambio di dati con i Comuni per l'allestimento del catalogo elettorale elettronico o la trasmissione dei risultati della votazione al servizio competente presso il Cantone.

Tutti i dati altamente sensibili di un'applicazione di voto si trovano nella cosiddetta «zona di alta sicurezza». Ne fanno parte, ad esempio, l'urna elettronica e il catalogo elettorale elettronico. La zona di alta sicurezza è protetta mediante firewall dalla rete dell'amministrazione ed è soggetta a forti limitazioni dell'accesso. Comprende, tra l'altro, gli elementi: costituzione del registro, rilascio di chiavi di identificazione e autenticazione, anonimato dei votanti, custodia dei voti nell'urna elettronica, controllo dei registri e determinazione dei risultati.

5.2.1.1 Catalogo elettorale virtuale

Per ognuna delle tre soluzioni previste, il catalogo elettorale virtuale costituisce l'inizio dei processi. I sistemi differiscono invece per quanto riguarda le loro condizioni. Il Cantone di Ginevra gestisce un registro abitanti centrale; nei Cantoni di Neuchâtel e Zurigo invece i registri degli abitanti sono gestiti dai Comuni. In tutti e tre i Cantoni i dati dei registri degli abitanti devono essere elaborati, in un giorno

⁷⁸ Per un elenco dettagliato delle misure di sicurezza adottate nei Cantoni pilota, cfr. la documentazione complementare 6; per una valutazione dettagliata delle misure di sicurezza cantonali, cfr. la documentazione complementare 5.

⁷⁹ PDA: Personal Digital Assistant sono piccoli dispositivi portatili che possono essere utilizzati per la memorizzazione di indirizzi, la gestione di termini ma anche per accedere a Internet.

prestabilito precedente la votazione o l'elezione, e raccolti in un catalogo elettorale temporaneo omogeneo necessario per allestire le carte di legittimazione e dotarle di indirizzo come pure per generare il codice di accesso e di autenticazione. Mediante parti di questo registro viene quindi generato il cosiddetto catalogo elettorale virtuale per il controllo della legittimazione durante la procedura di voto. I dati sono resi anonimi e ridotti ai contenuti necessari per il controllo dell'accesso per impedire che si possano stabilire nessi con i dati originali del singolo avente diritto di voto.

5.2.1.2 Carte di legittimazione

La produzione delle carte di legittimazione è delegata a tipografie che devono soddisfare elevate esigenze in materia di sicurezza. Le carte di legittimazione contengono, tra l'altro, i dati di accesso per annunciarsi al server di voto. In tutti i Cantoni, i codici di accesso sono stampati sulla carta di legittimazione.

Inoltre i votanti hanno bisogno di una parola d'ordine per l'autenticazione. I tre Cantoni hanno optato per tre soluzioni diverse: il Cantone di Ginevra nasconde la parola d'ordine sotto un campo da grattare. Il Cantone di Zurigo impiega un sistema analogo dato che la parola d'ordine è nascosta sotto un campo denominato «hydalam». Nel Cantone di Neuchâtel possono utilizzare il voto elettronico solo gli aventi diritto di voto iscritti al Guichet Unique. A queste persone la parola d'ordine di accesso per l'annuncio al Guichet Unique è comunicata con posta separata. Inoltre gli aventi diritto di voto neocastellani ricevono una lista di numeri simile alle liste di stralcio utilizzate nell'e-banking.

5.2.1.3 Identificazione, autorizzazione e validazione

Gli aventi diritto di voto si identificano al server di voto mediante il codice di accesso e la parola d'ordine che sono stati comunicati loro sulla carta di legittimazione. Altri approcci come l'identificazione attraverso un dialogo «challenge response» o l'impiego di smart card con firme digitali sono stati abbandonati dopo un esame approfondito nei Cantoni pilota. Le ragioni sono soprattutto la scarsa diffusione e l'insufficiente usabilità. Dopo l'identificazione, gli elettori sono abilitati a votare e dopo che hanno immesso le caratteristiche di voto, sono invitati a confermarle. Nei tre Cantoni, i procedimenti sono simili: il Cantone di Ginevra chiede l'immissione della data di nascita, del luogo di appartenenza e di un codice numerico di sei cifre. Nel Cantone di Zurigo è necessario immettere la data di nascita e un codice numerico di otto cifre. Nel Cantone di Neuchâtel la validazione dei voti avviene attraverso un codice numerico di sedici cifre. I voti sono immessi nell'urna elettronica solo dopo che la validazione è terminata con esito positivo.

5.2.1.4 Criptaggio e decriptazione dei voti

Per quanto riguarda le applicazioni pilota dei tre Cantoni si distinguono due fasi di criptaggio: una prima cifratura dei voti, delle caratteristiche di identificazione e di autenticazione avviene sul server client del relativo elettore. Si tratta di una normale chiave di cifratura a 128 bit (SSL) conforme allo standard di sicurezza del-

l'e-banking. I voti così criptati giungono via Internet nel settore protetto mediante firewall del sistema di voto elettronico (rete di amministrazione). Nei Cantoni di Zurigo e Ginevra, sono controllate la struttura e l'integrità dei valori ricevuti, quindi i valori sono nuovamente cifrati (almeno a 1024 bit) e trasferiti nella zona di alta sicurezza e nell'urna elettronica, dove restano conservati fino allo spoglio dei voti.

Nel Cantone di Neuchâtel, i voti criptati sono memorizzati direttamente nell'urna senza decrittazione e nuovo criptaggio. Oltre alla cifratura SSL i dati sono criptati nuovamente all'interno del canale. Anche il Cantone di Ginevra sta sperimentando un doppio criptaggio. Diversamente dai sistemi dei Cantoni di Ginevra e Zurigo, nel Cantone di Neuchâtel la verifica della struttura e dell'integrità del voto ha luogo solo al momento dello spoglio dei voti.

5.2.1.5 Sistema di memorizzazione ridondante

Tutti i dati dell'urna elettronica sono memorizzati contemporaneamente in sistemi ridondanti. I voti sono conservati in due banche dati collegate in parallelo e in due supporti di memorizzazione con memoria non volatile.

5.2.1.6 Verifica del diritto di voto nel seggio elettorale

In generale vi è il rischio che singoli aventi diritto di voto cerchino di votare sia elettronicamente che all'urna o per corrispondenza. Teoricamente questa possibilità sussiste perché, nell'ambito del voto elettronico, il materiale di voto fisico non viene ritirato. L'attuazione del voto elettronico può pertanto tangere i sistemi già applicati nel rispettivo Cantone e/o nel rispettivo Comune, ad esempio, per quando riguarda il controllo del diritto di voto nell'ambito del voto per corrispondenza o del voto all'urna.

Per ovviare a questo pericolo, le carte di legittimazione che inducono a pensare che il titolare abbia già votato per via elettronica devono essere verificate nei seggi elettorali e quando giungono per corrispondenza. Per la verifica, le carte di legittimazione sono state dotate di caratteristiche di sicurezza come i campi da grattare o i campi hydalam. Se una persona presenta ad esempio nel seggio elettorale una carta con un campo non intatto, si deve controllare nel catalogo elettorale elettronico se la persona non ha già votato elettronicamente.

A seconda della soluzione adottata e dell'organizzazione nel seggio elettorale, si possono svolgere le verifiche mediante interrogazione on line con PC o lettore a codice a barre, per telefono presso la centrale di voto o consultando un'apposita lista su cui sono indicate tutte le carte di legittimazione i cui detentori non hanno ancora votato.

Per l'ultimo sistema di verifica occorre tuttavia che l'urna elettronica venga chiusa prima dell'apertura dell'urna tradizionale. È quanto la Confederazione ha chiesto dai rispettivi Cantoni per tutte le prove pilota svolte in occasione di votazioni federali.

5.2.1.7 Verifica della plausibilità

Per la verifica della plausibilità dei risultati della votazione, le applicazioni pilota si basano su due metodi: da un lato viene effettuato un confronto quantitativo tra i codici di validazione qualificati come aventi diritto di voto e verbalizzati e il totale dei voti depositi nell'urna elettronica. Dall'altro, una commissione elettorale esprime voti di prova verbalizzati in modo dettagliato per un Comune virtuale. Questi voti sono trattati come tutti gli altri, ma non sono considerati nel conteggio del risultato totale. Il risultato della votazione del Comune virtuale viene quindi confrontato con il verbale. Per i due sistemi di verifica della plausibilità vale la tolleranza zero. Se non si riesce a raggiungere la tolleranza zero e se la causa dell'errore non può essere determinata in modo univoco e corretta in un secondo tempo, si deve partire dal presupposto che una falla del sistema o un attacco abbiano compromesso la votazione o l'elezione. Le autorità del Cantone interessato e della Confederazione devono quindi valutare se si può lo stesso determinare un risultato finale o se la votazione o l'elezione debba essere parzialmente o completamente ripetuta. Si deve anche decidere immediatamente se l'errore potrebbe avere un influsso su altre votazioni con voto elettronico, contemporanee o future.

5.2.1.8 Decrittazione dei voti

La decrittazione dei voti elettronici nei Cantoni di Ginevra e Neuchâtel può aver luogo solo sotto la sorveglianza di una commissione elettorale. Possono avviare il processo di decrittazione esclusivamente membri di questa commissione, che sono anche i soli a possedere le parole d'ordine e le chiavi necessarie. Per i casi d'emergenza provocati da cause di forza maggiore, la commissione affida le sue parole d'ordine, in busta sigillata, a un notaio affinché le custodisca dopo la loro attivazione e sino all'apertura dell'urna. Nel Cantone di Zurigo, invece, ogni Comune è autorizzato a attivare separatamente, mediante immissione della parola d'ordine e del numero della chiave, la decrittazione e il conteggio dei voti. Sia le parole d'ordine che le chiavi sono inviate ai Comuni per posta. Una chiave generale per i casi di emergenza è a disposizione del Cantone.

5.2.1.9 Sistema di determinazione dei risultati

Il Cantone di Ginevra ha un'autorità elettorale centrale. Qui i risultati dei voti elettronici, per corrispondenza e all'urna conteggiati per singolo Comune sono determinati centralmente dal Cantone. La determinazione dei risultati nei Cantoni di Zurigo e Neuchâtel, invece, è assicurata dai Comuni. I Comuni comunicano quindi i rispettivi risultati della votazione all'autorità cantonale competente.

5.2.1.10 Protezione dei dati

Nell'ambito dei progetti pilota di voto elettronico non sono stati elaborati dati personali di nessun genere a livello di Confederazione. Come per le modalità di voto tradizionali, la gestione del catalogo elettorale e la verifica dei diritti di voto hanno

avuto luogo esclusivamente nei Cantoni e nei Comuni. Con ogni probabilità questa prassi sarà mantenuta anche in caso di introduzione del voto elettronico. I Cantoni pilota hanno coinvolto gli incaricati cantonali della protezione dei dati nei lavori di preparazione e nello svolgimento delle prove pilota di voto elettronico. Dal punto di vista giuridico e politico, è necessario chiarire per tempo i contesti rilevanti in materia di protezione dei dati. L'Incaricato federale della protezione dei dati si è espresso in modo critico nei confronti del voto elettronico nei rapporti di attività del 2002 e del 2003⁸⁰. Il segreto del voto deve essere in ogni caso garantito. Dopo l'esame dei piani di sicurezza dei sistemi pilota cantonali da parte degli incaricati cantonali della protezione dei dati, l'Incaricato federale della protezione dei dati non si è più espresso criticamente sull'attuazione del voto elettronico.

5.2.2 Valutazione dell'attuazione cantonale con riferimento ai rischi

Al numero 3.2, i rischi tecnici del voto elettronico sono stati classificati in sei categorie di problemi. Nel seguito è presentata l'attuazione nell'ambito dei progetti pilota cantonali e sono valutati i rischi in base a una scala articolata su tre livelli (basso, medio alto).

5.2.2.1 Identificazione e autenticazione della persona avente diritto di voto

Dal punto di vista dell'autorità elettorale il problema è poter identificare e autenticare la persona avente diritto di voto per abilitarla a votare. In linea generale sono a disposizione diversi sistemi già affermati, per esempio numeri di identificazione e password personali, numeri di transazione, sistemi «challenge response» e/o certificati digitali. Perché gli utilizzatori accettino e impieghino un sistema è determinante anche il criterio dell'usabilità oltre a quello della sicurezza.

Nella fase progettuale, i Cantoni pilota hanno focalizzato l'attenzione sull'impiego di certificati digitali in forma di smart card. Purtroppo questi sistemi in Svizzera non sono ancora accessibili a tutti; le smart card con certificati digitali sono tuttora considerate prodotti di nicchia che vengono impiegati esclusivamente in ambienti altamente sensibili e con conseguenze finanziarie relativamente elevate. Nell'ambito dell'attuazione, i Cantoni si sono pertanto limitati a impiegare sistemi generalmente disponibili e meno costosi. Nel Cantone di Ginevra, la carta di legittimazione è stata completata con un campo da grattare che nasconde il codice di accesso. Nel Cantone di Neuchâtel, ai clienti che si sono iscritti al Guichet Unique viene inviata una lista di numeri con codici di transazione. Inoltre le persone aventi diritto di voto ricevono per posta una password separata e personale per ogni votazione. Nel Cantone di Zurigo, il codice di accesso è stampato sulla carta di legittimazione nascosto sotto un cosiddetto campo *hydalum*. Nello stesso tempo, in tutti e tre i Cantoni gli aventi diritto di voto devono dare indicazioni supplementari specifiche per persona (la data di nascita, il luogo di appartenenza) per essere abilitati al voto.

⁸⁰ Cfr. il 9° e il 10° rapporto di attività dell'Incaricato federale della protezione dei dati rispettivamente del 31 marzo 2002, pag. 14 seg., e del 31 marzo 2003, pag. 20 seg., www.edsb.ch/d/doku/jahresberichte/index.htm.

Il livello dei rischi per quanto riguarda l'identificazione e l'autenticazione della persona avente diritto di voto può essere considerato *basso*. Le soluzioni applicate offrono un grado di sicurezza sufficiente che può essere ulteriormente aumentato con l'adozione di sistemi che in futuro saranno disponibili e facili da usare.

5.2.2.2 Autenticazione del server di voto

Dal punto di vista della persona avente diritto di voto, il problema è assicurarsi di aver dato il voto al server giusto (cioè autentico). Server sbagliati potrebbero infatti cercare di intercettare le caratteristiche di identificazione di persone aventi diritto di voto. Le informazioni così acquisite potrebbero quindi essere utilizzate abusivamente. In questo contesto si parla spesso di «phishing». Purtroppo esempi del mondo dell'e-banking mostrano che molti cittadini sono troppo poco consapevoli di questi pericoli e rinunciano alle possibilità di verifica a disposizione. Vi è da temere che potrebbe essere così anche per il voto elettronico. Per tale motivo, questo è un settore altamente esposto ai rischi.

La maggior parte degli approcci a disposizione per difendersi da questi rischi ha per obiettivo il controllo parziale o integrale del software nell'apparecchio di immissione. Ciò si potrebbe ad esempio raggiungere con l'invio di un CD-ROM con sistema operativo e applicazione di voto elettronico. Gli aventi diritto di voto dovrebbero, prima di votare, caricare il CD-ROM nel proprio apparecchio. Dopo un esame approfondito, i Cantoni però hanno deciso di non adottare il sistema che non è di facile uso né tecnicamente semplice da installare negli apparecchi ottenibili sul mercato. Gli aventi diritto di voto ricevono invece, in ognuno dei tre Cantoni, la possibilità di verificare il certificato del server di voto attraverso un numero stampato sulla carta di legittimazione (impronta digitale del certificato). Inoltre nel corso della procedura di voto sono utilizzati codici o simboli trasmessi in forma grafica che gli aventi diritto di voto possono confrontare con i codici e i simboli che si trovano sulla carta di legittimazione.

I rischi relativi all'autenticazione del server di voto devono essere considerati medi perchè le misure di controllo descritte devono essere eseguite dai votanti stessi.

5.2.2.3 Comunicazione sicura

La comunicazione fra il sistema di computer di una persona avente diritto di voto e il server di voto deve essere assicurata crittograficamente per quanto riguarda la segretezza e l'integralità. A tal fine sono a disposizione il protocollo Secure Socket Layer (SSL) e il protocollo Transport Layer Security (TLS). L'impiego di uno di questi protocolli è conforme alla prassi per quanto riguarda le trasmissioni importanti dal punto di vista della sicurezza nell'ambito dell'e-banking ed è trasparente per l'utente. Sinora non sono noti problemi rilevanti di sicurezza e vulnerabilità del protocollo SSL/TLS. Mettendo in opera i loro sistemi, i tre Cantoni hanno integrato una trasmissione dei voti mediante il protocollo SSL. Il rischio di attacchi sul canale di comunicazione può pertanto essere considerato basso.

5.2.2.4 Sicurezza degli apparecchi di immissione

L'immissione dei voti nell'apposito apparecchio precede direttamente la trasmissione e deve essere considerata ad alto rischio. Senza essere riconosciuti, virus o cavalli di Troia potrebbero cercare di manipolare i voti scambiando, ad esempio, i sì e i no. In questo ambito, i sistemi crittografici non sono di aiuto. La problematica deve essere considerata altamente sensibile.

Virus e cavalli di Troia sono programmi indipendenti con una funzione devastatrice nascosta. Simili programmi possono inserirsi e diffondersi, spesso senza essere riconosciuti, nel sistema operativo di un computer (per esempio in forma di normale salvaschermo), procurare a terzi accesso a dati personali attraverso una porta secondaria, distruggere dati importanti o spiare le password. I virus e i cavalli di Troia rappresentano pertanto la più importante fonte di pericolo per il voto elettronico. Gli apparecchi terminali degli utenti sono al di fuori dell'ambito di influsso e di controllo delle autorità elettorali e di conseguenza la sicurezza di questi apparecchi non potrà mai essere garantita completamente. Per la trasmissione dei voti, i Cantoni pilota hanno comunque installato elementi di sicurezza che possono servire a impedire manipolazioni provocate da virus e cavalli di Troia. Le caratteristiche di voto immesse da una persona avente diritto di voto, ad esempio, sono trasmesse nuovamente per controllo all'avente diritto di voto prima che esprima il voto. Ciò non avviene in forma di testo, ma di immagine. È molto difficile che virus e cavalli di Troia riescano a riconoscere quest'immagine, che è manipolabile solo in condizioni molto complesse. Nel Cantone di Ginevra le immagini (sì, no, scheda bianca) sono anche dotate di un codice di quattro cifre. Il Cantone di Zurigo opera con simboli (p. es. di animali) invece che con codici. Inoltre le caratteristiche di voto, convertite in forma grafica sulla maschera di conferma, sono protette contro interventi manipolatori mediante linee serpeggianti unite. La persona avente diritto di voto può così verificare se l'informazione proviene dal server di voto o se è stata eventualmente modificata per vie traverse («attacco man-in-the-middle»). Il server di voto stesso verifica attraverso una somma di prova (valore hash), se il voto è stato modificato in una forma qualsiasi sul canale di trasmissione. Se è il caso, la procedura di voto viene interrotta dal lato del server. Il processo di voto verrebbe nuovamente eseguito dall'inizio. Si può così impedire, ma non escludere completamente, un cambiamento indesiderato e inosservato delle caratteristiche di voto. È presente un rischio medio.

5.2.2.5 Controllo democratico del processo di spoglio

Nell'ambito della procedura di voto tradizionale, il controllo democratico è assicurato da commissioni elettorali composte di persone aventi diritto di voto. Nella procedura elettronica, questi attori devono essere adeguatamente sostituiti, durante il periodo della votazione, con processi parziali controllati. Nei Cantoni pilota di Ginevra e Neuchâtel sono state costituite, con rappresentanti dei partiti politici e/o dei gruppi nel parlamento cantonale, commissioni elettorali che assistono all'apertura dell'urna elettronica e al conteggio dei voti elettronici. Nel Cantone di Zurigo le commissioni sono formate separatamente per ogni Comune. Le chiavi elettroniche che sono utilizzate per il criptaggio e la decriptazione dei voti elettronici sono protette mediante password delle commissioni. Si impediscono così gli accessi non autorizzati – anche da parte dell'autorità elettorale o addirittura degli amministratori del sistema (attacchi interni) – ai voti memorizzati in forma cifrata nell'urna. I rischi

delle varianti di soluzione attuate nei sistemi cantonali possono essere considerati bassi.

5.2.2.6 Tracciabilità e verificabilità

Secondo un'opinione ampiamente diffusa, ma problematica, la tecnologia di sicurezza impiegata nell'ambito dell'e-banking può essere utilizzata anche per il voto elettronico. In un punto centrale, l'e-banking e il voto elettronico differiscono in modo fondamentale: il primo richiede che le transazioni e le persone interessate siano registrate con precisione per eventuali controlli, il secondo esclude invece assolutamente queste registrazioni (protezione del segreto di voto). A causa della mancanza di tracciabilità e verificabilità, alcuni esperti mettono veementemente in dubbio il voto elettronico (audit trail). Diversamente dalle modalità di voto all'urna o per corrispondenza, nell'ambito del voto elettronico gli aventi diritto di voto non avrebbero la possibilità di assicurarsi che il loro voto è stato accettato correttamente dal server di voto e che se ne è tenuto conto nel conteggio. Inoltre, in modo diverso dalle procedure di voto tradizionali, l'autorità elettorale non avrebbe nessuna possibilità di accertare e perseguire un comportamento colpevole. A causa dell'assenza di un audit trail, il rischio deve essere considerato elevato. Il risultato del conteggio dei voti elettronici potrebbe essere messo in forse già solo se venisse asserito che sarebbero stati manipolati voti. In questo caso, per minimizzare i rischi, sarebbe assolutamente necessario preparare ed eventualmente adottare misure di comunicazione.

Quale possibile soluzione di tracciabilità individuale da parte di una persona avente diritto di voto è stato proposto da esperti il cosiddetto «Code-Voting»⁸¹: al posto delle caratteristiche di voto «sì», «no» o «scheda bianca» i votanti introducono le loro preferenze in forma di codice (p. es. «z3Gv» per «sì») nell'apparecchio di immissione. Il codice per ogni possibile caratteristica viene loro spedito prima individualmente con la carta di legittimazione. Il sistema di voto potrebbe quindi rispondere, per ogni voto ricevuto e espresso con sì, con un codice che la persona avente diritto di voto può verificare nella sua tabella dei codici prima di terminare l'operazione di voto. Questo procedimento presenta il chiaro vantaggio che il voto viene già immesso criptato individualmente e in più che viene confermato dal server in forma cifrata. Il cambiamento di medium (carta di legittimazione) rappresenterebbe in questo caso un ulteriore prezioso elemento di sicurezza. I Cantoni pilota si sono occupati intensamente della proposta nell'ambito della progettazione dei loro sistemi. Per il voto in Internet questa variante è stata tuttavia esclusa perché poco user friendly; è invece indispensabile per il voto mediante telefono cellulare perché in questo caso non possono essere svolti criptaggi dei voti in altra maniera. La forma criptata della trasmissione dei voti dall'apparecchio di immissione al sistema di voto è stata applicata con successo nell'ambito del voto zurighese con SMS.

In tal modo il problema dell'audit trail non è tuttavia ancora risolto. Non si ha ancora la certezza che il voto non sia stato cambiato o cancellato da un virus o cavallo di Troia lungo il percorso verso l'urna. Per questa ragione, altri esperti propongono di stampare ogni voto elettronico anche su carta al momento della votazione (paper trail), per consentire eventuali riconteggi su carta. Un'apposita stampante potrebbe

⁸¹ Cfr. per questa posizione Oppliger 2002b, pag. 24 seg. Per il riferimento bibliografico completo, cfr. la documentazione complementare 1.

essere installata in un safe chiuso a chiave presso gli impianti centrali ed essere così protetto contro accessi di terzi. La stampa su carta dei voti elettronici è richiesta attualmente da molti stati federali americani nell'ambito della certificazione delle macchine elettorali sviluppate per l'impiego nei seggi. Anche la Commissione di Venezia del Consiglio d'Europa ritiene la stampa su carta di ogni voto un utile complemento al voto elettronico (cfr. n. 4.4.1).

In caso di riconteggi, la stampa su carta dei voti potrebbe essere utilizzata quale riferimento per il confronto con il risultato determinato per via elettronica. Tuttavia, in questo caso la stampa dei voti su carta dovrebbe soddisfare esigenze di sicurezza molto elevate perché potrebbero essere infettati da virus e cavalli di Troia anche le stampanti e i computer che danno ordini di stampa facendo in modo che i voti figurino sulla stampa manipolati. Se i riconteggi dei voti elettronici e quelli dei voti stampati su carta dessero risultati diversi ci si dovrebbe chiedere quale voto considerare quello originale in caso di riconteggio. Logicamente, in questo caso un voto elettronico dovrebbe essere preso in considerazione solo nella sua forma elettronica a meno che non sia andato perso a causa di una distruzione generale delle memorie elettroniche ridondanti. Una situazione del genere potrebbe essere dovuta a causa di forza maggiore (catastrofe naturale), ma deve essere considerata improbabile.

Il procedimento paper trail non dovrebbe in nessun caso portare a consegnare alle persone aventi diritto di voto un giustificativo del voto che hanno effettivamente espresso. Il giustificativo del voto effettivamente espresso nelle mani di una persona avente diritto di voto non sarebbe infatti compatibile con l'articolo 281 CPS (corruzione elettorale) perché porrebbe essere utilizzato per l'acquisto o la vendita di voti. In questo caso l'esigenza di un paper trail per la rintracciabilità individuale si pone in contrasto con il diritto penale⁸².

Anche per il voto per corrispondenza o per quello all'urna, in ultima analisi, i criteri della tracciabilità e della verificabilità individuali non sono soddisfatti. Chi potrebbe verificare in modo univoco mediante ricorso che il proprio voto è stato registrato e contato correttamente? Le schede con un'annotazione, un nome o un simbolo qualsiasi devono essere considerate nulle sia in caso di votazioni popolari che di elezioni in quanto contengono contrassegni manifesti conformemente all'articolo 12 capoverso 1 lettera d, all'articolo 38 capoverso 1 lettera d e all'articolo 49 capoverso 1 lettera d della LDP. Nel presente rapporto abbiamo già rilevato che per quanto riguarda la sicurezza da garantire e la tracciabilità non ci si può aspettare dal voto elettronico più che dal voto tradizionale⁸³.

La soluzione del problema può essere cercata solo in una procedura che soddisfa l'esigenza di tracciabilità individuale attraverso un controllo democratico del processo elettorale (cfr. n. 5.2.2.5). Oltre all'impiego di commissioni elettorali con rappresentanti dei partiti politici che seguono il processo della votazione elettronica e generano e custodiscono le password necessarie al criptaggio e alla decrittazione, i Cantoni pilota impiegano uno strumento molto utile alla tracciabilità: la commissione costituisce un Comune di prova fittizio, che viene trattato dal sistema come

⁸² La stampa del voto espresso è stata esclusa esplicitamente nell'articolo 27h capoverso 4 dell'ODP (*«Il software utilizzato per l'elezione o la votazione non deve consentire di stampare il voto trasmesso»*). Sono fatti salvi disciplinamenti divergenti in via di ordinanza da parte del Consiglio federale, anche la possibilità dell'autorità elettorale di stampare il voto ad esempio quando giunge al server di voto.

⁸³ Cfr. n. 1.2

qualsiasi altro Comune politico del Cantone. I voti espressi nel Comune di prova seguono la stessa procedura dal momento della votazione alla decriptazione di tutti i voti elettronici. La commissione partecipa alla votazione con una determinata quantità di voti verbalizzati che tuttavia non sono considerati per la votazione. Dopo la decriptazione e il conteggio dei voti la domenica della votazione, il risultato del Comune di prova è confrontato con il verbale della Commissione. Si può così verificare se un errore del sistema o una manipolazione hanno provocato cambiamenti nei voti del Comune di prova. Se non è il caso, si può partire dal presupposto che con grandissima probabilità non è stata compromessa neanche l'integrità degli altri voti.

I rischi dovuti alla mancanza di tracciabilità e verificabilità devono essere considerati elevati. Mettendo in opera i progetti, i Cantoni pilota hanno sviluppato possibili soluzioni che, pur non realizzando la convalida individuale, consentono la convalida democratica dei risultati elettorali (chiavi crittografiche delle commissioni, Comuni di prova). Hanno così potuto ridurre i rischi a livelli accettabili. L'autorità responsabile deve comunque agire con la massima prudenza se l'opinione pubblica dovesse sostenere che sono stati manipolati voti.

5.2.3 Confronto con i rischi del voto per corrispondenza

Per valutare i rischi del voto elettronico si usa spesso come metro di paragone il voto per corrispondenza. Nella letteratura specialistica si trovano solo poche indicazioni sui rischi del voto per corrispondenza. Due studi si sono occupati parzialmente della questione⁸⁴. Von Arx giunge alla conclusione che gli abusi e le irregolarità (...) non si possono escludere completamente, ma che il voto per corrispondenza non costituisce un rischio sproporzionato⁸⁵. Nello studio dell'Università di Berna si afferma che spesso la volontà di aventi diritto di voto è falsata nella famiglia al momento della compilazione della scheda di voto. È soprattutto il marito che riempie anche la scheda della moglie; non capita invece mai che sia la moglie a compilare anche la scheda del marito⁸⁶. Lo studio non dà informazioni sulla frequenza degli abusi, ma giunge alla conclusione che gli abusi e le frodi rappresentano prevalentemente eventi rari e individuali. Secondo le Cancellerie comunali intervistate, il rischio di abusi nell'ambito del voto per corrispondenza è molto minore di quello nell'ambito del voto per rappresentanza.

Nel dicembre 2004 abbiamo affidato alla Cancelleria federale l'incarico di valutare i rischi del voto per corrispondenza e di confrontarli con i corrispondenti risultati dei progetti pilota di voto elettronico.

⁸⁴ Moser Christian, Hardmeier Sibylle e Linder Wolf. Unregelmässigkeiten bei erleichterter Stimmabgabe. Perizia commissionata dal Consiglio di Stato del Cantone Turgovia al Centro di ricerche in materia di politica svizzera dell'Università di Berna (Serie di pubblicazioni della Cancelleria di Stato del Cantone Turgovia n. 6), Turgovia 1990, pag. 12 segg.; Von Arx, Nicolas: Post-Demokratie, AJP, 1998, pag. 933-950, pag. 946 seg. Lo studio dell'università di Berna (= Moser et al. 1990) è stato realizzato dopo l'impugnazione di una votazione sulla Costituzione cantonale dalla quale era risultata una maggioranza estremamente esigua, cfr. anche DTF 114 Ia 42.

⁸⁵ Von Arx 1998, pag. 947

⁸⁶ Moser et al. 1990, pag. 29 seg., 65 e 69 segg.

In occasione della votazione popolare federale del 5 giugno 2005, la Cancelleria federale ha pertanto svolto un sondaggio sul voto per corrispondenza presso i Cantoni e, con l'aiuto delle Cancellerie di Stato, presso determinati Comuni scelti. Su richiesta della Conferenza Svizzera dei cancellieri di Stato, ha poi effettuato un ulteriore sondaggio in tutti i Comuni della Svizzera in occasione della votazione popolare federale del 27 novembre 2005⁸⁷.

I rischi del voto per corrispondenza nell'ambito del sondaggio del 5 giugno 2005 dovevano essere determinati rilevando da una parte le irregolarità e gli abusi effettivamente verificatisi⁸⁸ e dall'altra la percezione soggettiva dei rischi da parte dei Cantoni e dei Comuni.

Negli anni 2003/2004 vi sono stati nei Comuni intervistati in media 1,46 reclami su 1000 persone aventi diritto di voto. Nello stesso periodo di tempo è pervenuto ai Cantoni un numero inferiore di reclami (0,47 su 1000 aventi diritto di voto). La maggior parte dei reclami riguardava la perdita di carte di legittimazione e/o schede di voto. Al secondo posto figuravano le irregolarità dovute alla mancanza delle conoscenze necessarie da parte degli aventi diritto di voto.

Nettamente meno frequenti gli atti illeciti e gli abusi in relazione con il voto per corrispondenza: solo 2 Comuni su 60 (3,33 %) e 4 Cantoni su 24 (16,66 %) hanno fornito indicazioni in materia.

Dei 19 casi di irregolarità e di abusi verificatisi:

- 8 irregolarità erano dovute alla mancanza delle conoscenze necessarie da parte degli aventi diritto di voto;
- 7 irregolarità erano dovute a comportamenti errati da parte delle autorità elettorali;
- 4 casi di abuso e dolo.

Nella tabella seguente⁸⁹ si ricapitolano le esigenze e le misure di attuazione del voto elettronico derivanti da considerazioni di carattere giuridico e in materia di sicurezza mettendole a confronto con le esigenze e le misure analoghe nell'ambito del voto per corrispondenza.

⁸⁷ Cancelleria federale, sondaggi sul voto per corrispondenza svolti nel 2005 presso i Cantoni e i Comuni, Berna 2006 (cfr. la documentazione complementare 8).

⁸⁸ In questo contesto si intendono per irregolarità gli eventi accaduti casualmente per la mancanza delle conoscenze necessarie da parte degli aventi diritto di voto o delle autorità elettorali. Per abusi si intendono gli atti di dolo commessi intenzionalmente in relazione con il voto per corrispondenza.

⁸⁹ L'elenco si limita alle soluzioni sperimentate in Svizzera nell'ambito dei progetti pilota e non ha la pretesa di essere esaustivo.

Voto elettronico e voto per corrispondenza: confronto delle esigenze e delle misure di attuazione

| Esigenze del voto elettronico | Analogia(e) con il voto per corrispondenza | Misure nell'ambito dei progetti pilota |
|--|--|---|
| <p>Identificazione univoca: La persona che partecipa a una votazione o elezione deve essere identificata in modo univoco.</p> | <p>Gli aventi diritto di voto appongono la firma autografa sulla carta di legittimazione. Le schede devono essere riempite a mano.</p> | <ul style="list-style-type: none"> - Codice di accesso individuale e segreto - Indicazione della data di nascita e/o del luogo di appartenenza a fini di validazione - È previsto anche l'impiego di firme elettroniche - Problematiche sarebbero invece altre domande di sicurezza come il numero AVS (protezione del segreto di voto) |
| <p>Autenticità del sistema di voto elettronico: Gli aventi diritto di voto devono avere la garanzia che il loro voto è messo nell'urna giusta e preso in considerazione nel conteggio.</p> | <p>I voti per corrispondenza vengono recapitati per posta oppure sono portati al Comune o messi nella cassetta delle lettere comunale direttamente dai votanti.</p> | <ul style="list-style-type: none"> - Il certificato del server (SSL) può essere controllato tramite impronta digitale (fingerprint) dai votanti - L'autenticità del server può essere controllata mediante il codice della busta di trasmissione e/o mediante simboli di immagini |
| <p>Unicità del voto: Ogni avente diritto può esprimere soltanto un voto.</p> | <p>La carta di legittimazione è unico e personale. Chi vota per corrispondenza deve spedire la carta originale. In questo modo si impedisce che una persona possa votare due volte.</p> | <ul style="list-style-type: none"> - Immediata cancellazione della legittimazione nella banca dati del catalogo elettorale, non appena è stato registrato un voto (per via elettronica o corrispondenza) - Caratteristiche univoche sulla busta (p. es. integrità del sigillo sopra il codice di accesso segreto) indicano se un cittadino potrebbe già aver votato mediante voto elettronico |
| <p>Tutela del segreto di voto/protezione dei dati: La volontà della persona avente diritto di voto deve restare segreta; informazioni rilevanti dal punto di vista della protezione dei dati non devono giungere a terzi.</p> | <p>Le schede compilate giungono al Comune chiuse in busta separata. Dopo il controllo della validità delle firme, la carta di legittimazione e il voto devono essere messi in urne separate.</p> | <ul style="list-style-type: none"> - Memorizzazione di dati personali e caratteristiche di voto in sistemi diversi - Un «generatore di numeri casuali» provvede a mischiare regolarmente il contenuto dell'urna elettronica per impedire che p. es. in base all'ordine di entrata dei voti si possa risalire ai votanti |

| Esigenze del voto elettronico | Analogia(e) con il voto per corrispondenza | Misure nell'ambito dei progetti pilota |
|--|--|---|
| <p><i>Misure contro i rischi di forza maggiore:</i> Possono compromettere lo svolgimento di votazioni e elezioni il maltempo, le interruzioni di corrente, i terremoti ecc.</p> | <p>Pericoli analoghi esistono anche per i municipi, le cassette delle lettere comunali, i seggi elettorali, i centri postali e le vie postali. Nell'ambito del voto elettronico può però essere interessata una quantità maggiore di voti.</p> | <ul style="list-style-type: none"> - Gestione di diversi server ridondanti - Sistemazione dei server in edifici di alta sicurezza (controllo dell'accesso, protezione antincendio, gruppo elettrogeno di emergenza) |
| <p><i>Rintracciabilità e verificabilità:</i> In caso di decisione popolare con maggioranza esigua o di ricorso, si deve poter procedere al riconteggio dei voti.</p> | <p>Il riconteggio dei voti su supporto cartaceo è possibile in qualsiasi momento. Per il riconteggio si possono convocare altre persone. Su richiesta, i cittadini possono assistere al riconteggio (trasparenza).</p> | <ul style="list-style-type: none"> - Allestimento di verbali convenzionali ed elettronici firmati dalle autorità competenti al momento dello spoglio dei voti - Allestimento di un supporto dati separato (CD-ROM con il contenuto dell'urna elettronica e tutti i log-file) - La rappresentanza degli aventi diritto di voto è assicurata da controllori designati dai partiti politici |
| <p><i>Fiducia:</i> Tutta la procedura deve ispirare fiducia ed essere verificabile.</p> | <p>Il voto per corrispondenza gode della fiducia della popolazione.</p> | <ul style="list-style-type: none"> - Integrazione dei controllori in tutti i processi sensibili - Verifica indipendente del codice sorgente, metodo open source - Trasparenza di applicazioni proprietarie |
| <p><i>Difesa contro attacchi esterni:</i> a) Apparecchi terminali d'utente (computer privati, telefoni cellulari): possibilità di intercettare e modificare i voti, p. es. mediante cavalli di Troia</p> | <p>Il materiale di voto viene sottratto dalla cassetta delle lettere di una persona avente diritto di voto. Non si possono escludere abusi sistematici se molti aventi diritto di voto che non votano gettano il materiale di voto senza strapparlo.</p> | <ul style="list-style-type: none"> - Protezione multipla mediante firewall - Sistema di Code-Voting (SMS Zurigo, trasmissione del voto in Internet in forma di codice numerico) - Impiego di software antivirus attuali |
| <p>b) Canale di comunicazione («tra-sporto» del voto dall'utente al server): possibilità di intercettare e modificare i voti (attacchi man-in-the-middle).</p> | <p>Perché sottratte dalla cassetta delle lettere comunale oppure per furto o perdita di un sacco postale, le buste potrebbero finire nelle mani di persone non autorizzate oppure essere distrutte.</p> | <ul style="list-style-type: none"> - Il voto viene criptato (SSL) - Le caratteristiche di voto sono trasmesse in forma grafica e non in forma di testi - In forma dialogica è controllata l'integrità di tutti i pacchetti mediante somme orizzontali |

| | | |
|---|---|--|
| Esigenze del voto elettronico | Analogia(e) con il voto per corrispondenza | Misure nell'ambito dei progetti pilota |
| c) Piattaforma (centro vitale di un sistema di voto elettronico): ad esempio «attacchi denial-of-service» | Attacco incendiario alla cassetta delle lettere del Comune. Oppure la Posta non riesce a recapitare i voti a causa di gravi disagi. Il rischio è piccolo, ma aumenta più viene centralizzato il servizio postale. | <ul style="list-style-type: none"> – Gestione di diversi server ridondanti – Collaborazione con diversi provider (contro il DNS-Hacking) |

5.3 Economicità e fattibilità

5.3.1 Costi dei progetti pilota

Nei contratti con i tre Cantoni di Ginevra, Neuchâtel e Zurigo, la Confederazione Svizzera, rappresentata dalla Cancelleria federale, si è impegnata ad assumere al massimo l'80 per cento dei costi supplementari che i progetti pilota provocano rispetto a votazioni o elezioni normali.

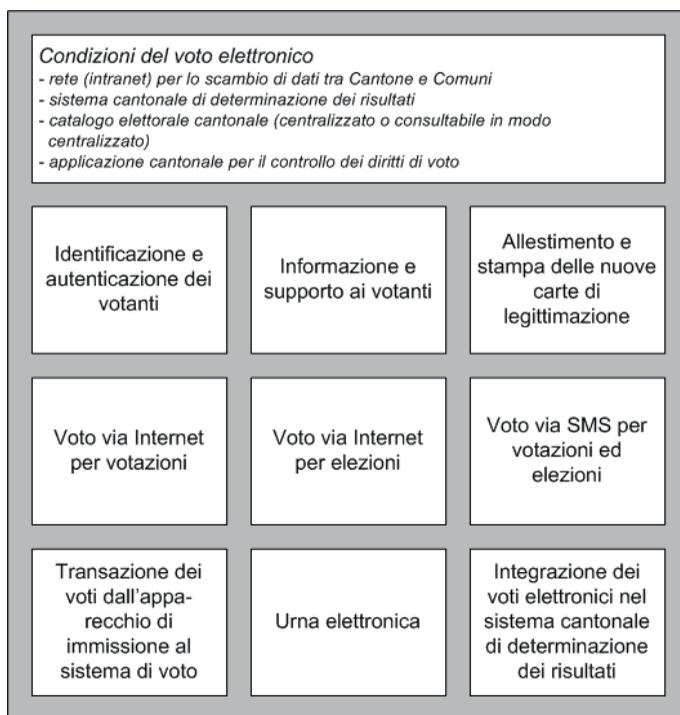
La Confederazione si è assunta, in particolare, i costi necessari per la progettazione della necessaria architettura di sicurezza. Le spese per il personale impiegato nei Cantoni sono state sopportate dai Cantoni stessi. Con lo svolgimento delle prime prove pilota in occasione di votazioni popolari federali sono state fornite per la fine del 2005 le prestazioni che la Confederazione e i Cantoni avevano convenuto per contratto.

A causa delle rispettive condizioni diverse per l'introduzione del voto elettronico, i Cantoni hanno adottato soluzioni specifiche per quanto riguarda la struttura del sistema. I Cantoni di Ginevra e Neuchâtel ad esempio hanno potuto ricorrere a dati di registri già disponibili in rete per allestire un catalogo elettorale cantonale per ogni evento; il Cantone di Zurigo, invece, per sviluppare il suo sistema ha dovuto prima realizzare questa messa in rete. Nel Cantone di Neuchâtel, il voto elettronico è stato concepito come elemento di un portale integrale dell'amministrazione (Guichet Unique); i Cantoni di Zurigo e di Ginevra mettono invece a disposizione piattaforme alle quali è possibile accedere direttamente.

Anche per quanto riguarda la quantità di moduli da realizzare si possono riscontrare notevoli differenze tra i progetti pilota. I Cantoni di Neuchâtel e di Ginevra hanno sviluppato moduli per votare via Internet. Nel Cantone di Zurigo è stata presa in considerazione nell'ambito del progetto pilota anche la tecnologia SMS ed è stato sviluppato un sistema di gestione integrato di votazione ed elezione con interfacce verso il sistema di determinazione dei risultati già disponibile denominato WABSTI⁹⁰. Anche i costi dei tre progetti pilota differiscono notevolmente a causa di queste differenti condizioni ed è pertanto difficile operare confronti da questo punto di vista.

⁹⁰ WABSTI: Sistema di votazione ed elezione dei Cantoni Turgovia, San Gallo, Soletta e dei Grigioni.

Struttura modulare di un sistema di voto elettronico



Alla fine della fase di sviluppo nel 2005, la Cancelleria federale ha rilevato i costi complessivi dei singoli progetti pilota (inclusi i costi di personale non sopportati dalla Confederazione). Le tabelle dei costi per ogni Cantone pilota si trovano nella documentazione complementare 3. Nella tabella che segue sono riportati i costi dei progetti che la Confederazione ha contribuito a sostenere:

Costi dei progetti dei Cantoni pilota che la Confederazione ha contribuito a sostenere

| Cantone | Costi del progetto | Osservazioni |
|-----------|--------------------|--|
| Ginevra | 740 000 fr. | Costi di infrastruttura |
| | 2 728 800 fr. | Costi di sviluppo |
| | 337 122 fr. | Perizie |
| | 1 498 500 fr. | Costi di esercizio |
| Neuchâtel | 3 500 000 fr. | Sviluppo del Guichet Unique, con modulo di identificazione |
| | 2 300 000 fr. | Sviluppo del Guichet Unique, senza modulo di identificazione |
| Zurigo | 2 652 015 fr. | Sviluppo del voto elettronico, senza costi di progettazione |
| | 2 867 586 fr. | Costi di progettazione |

Alla fine del 2005, la Cancelleria federale aveva contribuito, nell'ambito dei suoi impegni contrattuali, con complessivi 5,96 milioni di franchi alle spese di sviluppo e ai costi dei progetti pilota cantonali direttamente legati alle prove pilota:

| | |
|-----------------------|---------------|
| Cantone di Ginevra: | fr. 1 410 000 |
| Cantone di Neuchâtel: | fr. 2 227 000 |
| Cantone di Zurigo: | fr. 2 323 000 |

Totale contributi erogati dalla Cancelleria federale fr. 5 960 000

La Cancelleria federale non ha potuto soddisfare tutte le richieste di finanziamento dei Cantoni pilota. Ha però rispettato gli impegni finanziari previsti nei contratti e nelle convenzioni. Il Controllo federale delle finanze ha confermato nell'ottobre 2005 la validità del finanziamento e della gestione dei progetti⁹¹. Se si tiene conto delle spese di personale sostenute durante la fase pilota nella Cancelleria federale e delle spese per i gruppi di lavoro e di monitoraggio di complessivi 1 135 400 franchi, dei pagamenti per progetti di terzi (identificatore delle persone, identità digitale) di 277 664 franchi come pure dei costi di 153 005 franchi sostenuti prima delle prove per perizie sulla sicurezza e dei costi di 51 502 franchi per sondaggi svolti nell'ambito della ricerca scientifica concomitante, la Confederazione ha sostenuto, negli anni 2000–2005, una spesa complessiva di 7 577 571⁹² franchi per il progetto di voto elettronico.

⁹¹ Controllo federale delle finanze, E-Government und NOVE-IT in der Bundeskanzlei, Berna, ottobre 2005, www.efk.admin.ch/pdf/5015BE_VE_GV_v02_Version_Publikation_17112005.pdf.

⁹² Le spese sono state, nel 2001: 938 742 franchi; nel 2002: 1 103 371 franchi; nel 2003: 1 042 773 franchi; nel 2004: 4 146 695 franchi e nel 2005: 345 990 franchi.

5.3.2

Costi dell'introduzione del voto elettronico

Nel nostro rapporto sul voto elettronico del 9 gennaio 2002 abbiamo stimato a 400–620 milioni di franchi i costi per l'introduzione capillare del voto elettronico e un esercizio della durata di dieci anni⁹³. Ora, dopo che i sistemi di voto elettronico sono stati sviluppati nei Cantoni di Ginevra, Zurigo e Neuchâtel, i costi sostenuti per i progetti negli anni 2000–2005 e consistenti in sussidi federali devono essere documentati e la stima del 2002 deve essere messa a confronto con i valori effettivi rilevati.

Il Cantone che decide di gestire un sistema di voto elettronico deve sostenere costi di investimento o di implementazione relativamente elevati per la costruzione o la ripresa del sistema e costi ricorrenti annui di manutenzione e di perfezionamento (ammortamento incluso).

Tabella 4

Costi complessivi calcolati per lo sviluppo di un vasto sistema di voto elettronico compresi i costi per un esercizio della durata di 10 anni⁹⁴

| | |
|--|-----------------------|
| Costi di sviluppo (unici) | fr. 5 763 115 |
| A. Costi d'investimento | |
| Hardware con rete | fr. 702 492 |
| Software | fr. 176 894 |
| Costi per lo sviluppo del sistema | fr. 1 745 629 |
| B. Costi di progetto | |
| Costi di progettazione | fr. 2 867 586 |
| Costi di test | fr. 253 714 |
| Collaudo del sistema (omologazione) | fr. 16 800 |
| Costi ricorrenti (calcolati per 10 anni) | fr. 4 925 000 |
| Licenze per banche dati, sistemi operativi, ammortamento hardware e nuovi investimenti, housing, provider SMS, amministrazione, aggiornamenti software, supporto, confronto dei cataloghi elettorali, layout di maschere, gestione banche dati | |
| Maggior onere per votazioni (calcolato per 10 anni) | fr. 4 672 000 |
| Installazione degli apparecchi tecnici nei seggi elettorali, carta e stampa, costi di personale per helpdesk, supporto, costi di personale per controllo | |
| Costi complessivi per i primi 10 anni | fr. 15 360 115 |

⁹³ FF 2002 608 seg.

⁹⁴ I costi dell'introduzione sono calcolati, per i tre progetti, sulla base del progetto di Zurigo (per indicazioni dettagliate sulle tabelle riassuntive cantonali dei costi, cfr. la documentazione complementare 7). La limitazione al sistema di Zurigo è giustificata: questo sistema costituisce la soluzione più completa e costosa delle varianti nei tre Cantoni pilota.

I costi per lo sviluppo e l'esercizio di un vasto sistema di voto elettronico per 10 anni generano pertanto costi complessivi di circa 15,36 milioni di franchi. Sono compresi anche tutti i costi di personale e servizio calcolati in modo esplorativo. Il sistema è configurato per almeno 800 000 aventi diritto di voto.

Calcolato per un esercizio di 10 anni un simile sistema provocherebbe ogni anno costi di 1 536 012 franchi, corrispondenti a un importo di 384 003 franchi per una votazione (stima: 4 votazioni all'anno). Più sono gli aventi diritto di voto che possono utilizzare il voto elettronico, più sono economici gli investimenti e i costi di manutenzione:

Tabella 5

Esempio di variazione dei costi in funzione del numero di aventi diritto di voto

| | |
|------------------------------------|-------------------------------|
| Per 50 000 aventi diritto di voto | fr. 7,68 per ogni voto |
| Per 100 000 aventi diritto di voto | fr. 3,84 per ogni voto |
| Per 250 000 aventi diritto di voto | fr. 1,54 per ogni voto |
| Per 500 000 aventi diritto di voto | fr. 0,77 per ogni voto |
| Per 800 000 aventi diritto di voto | fr. 0,48 per ogni voto |

Si deve anche precisare che, tranne quello di Zurigo, nessun Cantone può usufruire di un prezzo così basso per singolo voto. Per Cantoni con un numero inferiore di aventi diritto di voto, lo sviluppo e l'esercizio di un simile sistema non riuscirebbero a soddisfare criteri economici.

Se tutti e 26 i Cantoni svizzeri realizzano ed esercitano, senza nessun trasferimento di know how dai Cantoni pilota, un proprio sistema di voto elettronico, i costi complessivi sono stimati a quasi 400 milioni di franchi⁹⁵. Se invece i Cantoni gestiscono in comune uno o più sistemi, i costi si riducono notevolmente. Il sistema qui descritto è concepito per almeno 800 000 aventi diritto di voto. Se si gestisce un solo sistema in Svizzera, i costi di 5,76 milioni di franchi devono essere sostenuti una sola volta. I costi ricorrenti annui per ammortamenti, manutenzione e nuovi investimenti ammontano in questo caso a circa 1 milione di franchi per ogni 800 000 persone aventi diritto di voto. La Svizzera comprende, con 4,85 milioni di aventi diritto di voto, circa sei volte la quantità indicata; di conseguenza si possono stimare a 65,76 milioni di i costi minimi per l'introduzione capillare del voto elettronico⁹⁶. Se invece gruppi di 4–5 Cantoni impiegano, indipendentemente dagli altri gruppi, in totale 6 sistemi, i costi ammontano a 92,16 milioni di franchi. I costi di sviluppo già sostenuti dai Cantoni pilota e dalla Confederazione non sono presi in considerazione

⁹⁵ Se in Svizzera venissero costruiti 26 sistemi indipendenti come quello del Cantone di Zurigo, si dovrebbero prevedere a livello svizzero per un esercizio di 10 anni costi d'investimento e di esercizio di oltre 399 milioni di franchi ($26 \times 15,36$ milioni di franchi). Già nel 2002 avevamo stimato a 400–620 milioni di franchi i costi per l'introduzione capillare del voto elettronico e un esercizio decennale (FF 2002 608).

⁹⁶ Questo importo comprende costi unici di sviluppo di 5,76 milioni di franchi e costi annui ricorrenti e oneri supplementari annui per un totale di 1 milione di franchi per ogni 800 000 aventi diritto di voto (cfr. tabella 4). La stima dei costi ricorrenti e degli oneri supplementari si basa sul totale dei cittadini svizzeri aventi diritto di voto (4,85 milioni) per un periodo di 10 anni.

in questi calcoli perché si dovrebbero sostenere costi di implementazione dello stesso ordine di grandezza.

Per lo stesso periodo di tempo si stimano a circa 252,61 milioni di franchi i costi complessivi del voto per corrispondenza. È quanto risulta da un rilevamento della Cancelleria federale presso i Cantoni e i Comuni in occasione della votazione popolare federale del 5 giugno 2005⁹⁷.

Il voto elettronico può dunque essere realizzato in modo notevolmente più economico di quello per corrispondenza. La condizione tuttavia è che più Cantoni gestiscano un sistema in comune e trasferiscano i processi propri a tutte le varianti di voto (come la stampa delle carte di legittimazione, l'allestimento del catalogo elettorale, il controllo dei diritti di voto ecc.) in un sistema di votazione ed elezione integrale.

5.3.3 Potenziale di risparmio

L'introduzione capillare del voto elettronico a complemento del voto tradizionale permetterebbe di fare ulteriori risparmi. Un notevole potenziale di risparmio si registra nell'ambito delle risorse di personale (minor onere per controllare i diritti di voto, per ricevere e conteggiare i voti per corrispondenza), ma anche per quanto riguarda le spese per la spedizione delle buste di trasmissione dei voti per corrispondenza. Secondo un sondaggio svolto nel giugno 2005 su incarico della Cancelleria federale presso i Cantoni e i Comuni⁹⁸ la parziale sostituzione dei voti per corrispondenza con voti elettronici permette di risparmiare circa 1,61 franchi per persona avente diritto di voto.

⁹⁷ Cancelleria federale, sondaggi sul voto per corrispondenza svolti nel 2005 presso i Cantoni e i Comuni, Berna 2005 (cfr. la documentazione complementare 8). La spesa media per un voto per corrispondenza ammonta a fr. 3.65. Nei costi di un voto per corrispondenza sono compresi costi fissi medi di porto ecc. di fr. 1.45 e costi proporzionali di fr. 2.20 per il conteggio dei voti ecc. Per il calcolo ci si è basati su quattro votazioni all'anno. Calcoli basati su 4 860 166 aventi diritto di voto (27.11.2005), su una partecipazione al voto del 44,5 % (CH: 1996–2005) e una percentuale dell'80 % di voti per corrispondenza.

⁹⁸ Ibidem

Stima dei minori costi in caso di introduzione del voto elettronico in Svizzera*In centesimi per ogni voto espresso per via elettronica invece che per corrispondenza*

| | centesimi |
|--|-------------|
| Risparmio sulle spese di materiale | |
| Spese di porto per la trasmissione dei voti per corrispondenza (valore medio svizzero delle spese di porto sostenute dallo Stato) | 40,0 |
| Spese per la conservazione dei voti per corrispondenza (affitto locali, spese di materiale) | 11,9 |
| Conteggio dei voti per corrispondenza (affitto locali, spese di materiale, senza spese di personale) | 10,1 |
| Altre spese nell'ambito del voto per corrispondenza | 8,1 |
| Totale risparmio sulle spese di materiale | 70,1 |
| Risparmio sulle spese di personale | |
| Ricezione e conservazione dei voti, controllo dei diritti di voto | 24,8 |
| Conteggio dei voti (a mano o a macchina) | 49,1 |
| Altro | 17,3 |
| Totale risparmio sulle spese di personale | 91,2 |

In caso di impiego del voto elettronico, le spese di spedizione dei voti per corrispondenza non devono più essere sostenute nei Cantoni e nei Comuni in cui sono gli aventi diritto di voto a pagarle.

Nel caso di una quota dell'8,9 per cento⁹⁹ di voti elettronici sul totale dell'elettorato svizzero, il potenziale di risparmio ammonta a 27,86 milioni di franchi per un esercizio della durata di 10 anni.

Complessivamente, dunque, i costi per l'introduzione capillare del voto elettronico in Svizzera possono essere stimati a 37,90 fino a 64,30 milioni di franchi – a condizione che tra i Cantoni si instauri un'ampia collaborazione¹⁰⁰.

⁹⁹ Base: una partecipazione media al voto del 44,5 % (CH: 1996–2005), una quota media dell'80 % di votanti a distanza, il 25 % dei quali per via elettronica, e 4 votazioni all'anno.

¹⁰⁰ I due valori risultano dalla differenza tra le spese per lo sviluppo e l'esercizio di un solo sistema per tutti i Cantoni e per lo sviluppo di sei corrispondenti sistemi (cfr. n. 5.3.2) e il potenziale di risparmio uguale per le due varianti (cfr. n. 5.3.3).

5.3.4 Due varianti di collaborazione tra i Cantoni

In Svizzera, l'esercizio di 26 diversi sistemi non è sostenibile dal punto di vista economico.

Per contro è razionale procedere congiuntamente: le soluzioni sviluppate nei Cantoni pilota possono essere utilizzate da ulteriori Cantoni, a condizione che vi sia la necessaria volontà politica.

Sulla base di considerazioni economiche e politiche si possono ipotizzare due varianti¹⁰¹:

- la prima consiste nel trasferimento tecnologico da un Cantone all'altro. I Cantoni pilota si sono impegnati nei contratti con la Cancelleria federale al trasferimento gratuito delle conoscenze e della tecnologia dei componenti sviluppati con i contributi finanziari della Confederazione;
- la seconda consiste nella possibilità che i Cantoni riprendano un sistema esistente¹⁰².

L'introduzione di un sistema di voto elettronico comune potrebbe però anche tangere le attuali diversità cantonali. Negli anni passati, i Cantoni svizzeri hanno realizzato sistemi di voto elettronico facilmente utilizzabili e vicini al cittadino. La varietà e singolarità andrebbero parzialmente perse in caso di una maggiore collaborazione nell'ambito del voto elettronico. I Cantoni dovrebbero decidere quali elementi del loro sistema di votazione ed elezione vorrebbero in ogni caso mantenere e con quali altri sistemi cantonali potrebbero immaginarsi una collaborazione. A causa dei canali di trasmissione elettronici, in questo caso più che la vicinanza contano le analogie fra i sistemi.

5.3.5 Armonizzazione dei cataloghi elettorali e identificatore delle persone

La disponibilità di un identificatore delle persone a livello federale non è una condizione essenziale per svolgere con successo votazioni ed elezioni elettroniche in Svizzera come l'armonizzazione a livello cantonale dei cataloghi elettorali gestiti per singolo Comune o l'allestimento di un catalogo elettorale elettronico prima di ogni votazione.

Nonostante ciò, un identificatore uniforme valido in Svizzera per tutti i registri delle persone potrebbe semplificare l'introduzione del voto elettronico. In particolare, un sistema di notificazione più efficiente in caso di trasloco da un Cantone all'altro potrebbe impedire che in futuro una persona possa ricevere per sbaglio il materiale di voto dei due Cantoni a causa di scadenziari diversi.

¹⁰¹ La gestione da parte della Confederazione di un sistema centrale per tutti i Cantoni rappresenterebbe tecnicamente un'ulteriore possibilità, ma non sarebbe praticamente realizzabile nel sistema federalistico della Svizzera e non è stata pertanto presa in considerazione nel presente rapporto.

¹⁰² Una standardizzazione delle interfacce rilevanti per il voto elettronico tra registri degli abitanti e cataloghi elettorali a livello comunale e cantonale e della trasmissione dei dati dei moduli di voto elettronico tra loro favorirebbe ancora di più questa variante.

Il 27 ottobre 2004 abbiamo incaricato il DFI di elaborare le basi legali per l'armonizzazione dei registri delle persone e per l'istituzione di un identificatore delle persone uniforme per i registri delle persone.

Il 23 novembre 2005 abbiamo ha adottato i disegni elaborati nell'ambito del messaggio sull'armonizzazione dei registri ufficiali di persone (FF 2006 397) proponendo contemporaneamente di sostituire gli attuali numeri AVS con numeri di assicurazione sociale di 13 cifre «non parlanti» (non esprimenti caratteristiche). Questi numeri hanno funzioni diverse: possono ad esempio essere impiegati quali identificatori delle persone in tutti i registri della popolazione. Nel registro degli abitanti deve essere documentato anche il diritto di votazione ed elezione, cosa che può essere sfruttata per la generazione di cataloghi elettorali. Un catalogo delle caratteristiche per la gestione dei registri degli abitanti per i Cantoni e i Comuni è stato pubblicato nel settembre 2005 dall'Ufficio federale di statistica¹⁰³.

5.4 Considerazioni conclusive e ulteriore procedura

Da un sondaggio svolto a livello nazionale risulta che il progetto di voto elettronico è conosciuto da due terzi degli intervistati. Oltre la metà degli intervistati afferma che intende utilizzare il voto elettronico quando sarà a disposizione. Oltre il 90 per cento degli aventi diritto di voto che hanno partecipato effettivamente alle prove pilota e utilizzato il voto elettronico per votare vorrebbe continuare a utilizzare questa forma di voto. Gli aventi diritto di voto sono molto sensibili nei confronti della sicurezza del voto elettronico oltre che verso l'usabilità che viene citata regolarmente negli studi collaterali.

Nell'ambito dei progetti pilota in materia di voto elettronico sono state sperimentate numerose misure di sicurezza atte a affrontare efficacemente i rischi di un abuso sistematico del voto elettronico¹⁰⁴. Come per le modalità di voto tradizionali all'urna o per corrispondenza anche per il voto elettronico non si potrà mai escludere completamente che singoli voti possano essere, accidentalmente o illecitamente, falsificati, manipolati o impediti o che persone non autorizzate possano osservare come votano singole persone. In ogni caso però si deve poter impedire che simili irregolarità e abusi possano verificarsi sistematicamente.

Le misure di sicurezza adottate hanno permesso di difendersi efficacemente contro attacchi effettivamente eseguiti. Esperti esterni hanno attestato un'architettura di sicurezza molto buona ai tre progetti. La sicurezza raggiunta dagli impianti centrali (urna, server di voto, cataloghi elettorali) è paragonabile a quella di complesse applicazioni di e-banking delle grandi banche svizzere. Secondo gli obiettivi fissati dalle Camere federali per il progetto, le misure di sicurezza dovevano assicurare al voto elettronico almeno lo stesso livello di sicurezza del voto per corrispondenza. Questo valore indicativo è stato addirittura superato.

¹⁰³ UST, l'armonizzazione dei registri ufficiali di persone, dei registri cantionali e comunali degli abitanti, catalogo ufficiale delle caratteristiche, Neuchâtel 2005 (BFS, Die Harmonisierung amtlicher Personenregister, kantonale und kommunale Einwohnerregister, Amtlicher Katalog der Merkmale, Neuchâtel 2005).
www.bfs.admin.ch/bfs/portal/de/index/infotek/erhebungen_quellen/statistik_und_register/registerharmonisierung/publikationen.Document.65357.html.

¹⁰⁴ Per il quadro sinottico delle misure di sicurezza tecniche realizzate nell'ambito dei progetti pilota cantionali, cfr. la documentazione complementare 6.

La Cancelleria federale e i Cantoni pilota hanno utilizzato in modo economico i mezzi finanziari messi a disposizione per i progetti pilota. I tre sistemi sono stati costruiti in modo da resistere al tempo e sono attrezzati per impieghi futuri. In caso di introduzione capillare del voto elettronico in Svizzera, i costi per un periodo di dieci anni sono stimati a 65,76 milioni di franchi per un sistema unico per tutti i Cantoni, a 92,16 milioni di franchi per 6 sistemi diversi e fino a 400 milioni di franchi per soluzioni cantonali individuali. A questi costi si contrappone un potenziale di risparmio di 27,86 milioni di franchi nell'ambito del voto per corrispondenza. L'introduzione del voto elettronico in tutta la Svizzera provocherebbe, di conseguenza, costi netti minimi di 37,90 e massimi di 400 milioni di franchi. La maggior parte dei costi sarebbe a carico dei Comuni e dei Cantoni. Per il resto non si possono prevedere ripercussioni di rilievo sull'economia. La gestione della campagna elettorale presso i partiti, le associazioni e i gruppi di interesse è già cambiata in modo radicale, cioè con un prolungamento della durata della votazione, con l'introduzione del voto per corrispondenza. Il voto elettronico è offerto nello stesso periodo di tempo in cui si può votare per corrispondenza e non provoca quindi ulteriori dilatazioni. Unicamente nell'ambito della propaganda politica potrebbero verificarsi spostamenti da media stampati e invii postali a media elettronici e trasmissioni elettroniche, dato che Internet suscita maggiore interesse quale piattaforma per la campagna. La stessa evoluzione è in atto anche al di fuori dell'ambito dei diritti politici.

I progetti pilota hanno provato la fattibilità del voto elettronico in Svizzera. I sistemi pilota stessi, parti (moduli) di essi e il know how acquisito durante la sperimentazione sono messi a disposizione, in massima parte gratuitamente, dei Cantoni interessati. I Cantoni pilota e altri Cantoni sono disposti ad estendere i progetti pilota gradualmente a tutto il territorio del Cantone e anche a elezioni. A questo proposito dovrebbe però intervenire la Confederazione definendo direttive strategiche per la procedura da seguire e adeguando le basi giuridiche.

5.4.1 Realizzazione graduale

È utile precisare ancora più dettagliatamente la suddivisione in tappe¹⁰⁵ proposta nel nostro primo rapporto del 9 gennaio 2002 sul voto elettronico. La prima tappa di prove controllate del voto elettronico deve essere ampliata in modo che si possono acquisire ulteriori esperienze. In particolare, i tre Cantoni che hanno introdotto il voto elettronico ed effettuato notevoli investimenti devono poter continuare a svolgere progetti pilota. Si prevede che ulteriori Cantoni interessati possano partecipare alle prove senza il contributo finanziario della Confederazione. In particolare è molto importante evitare che si crei un divario digitale tra Cantoni urbani o grandi e Cantoni periferici o piccoli. Dato che irregolarità nell'ambito del voto elettronico, voci su presunte irregolarità e abusi all'estero che potrebbero minare la fiducia nel voto elettronico rischiano di compromettere la credibilità di votazioni ed elezioni federali in generale, il Consiglio federale provvederà nell'ambito delle sue autorizzazioni a fare in modo che nel corso della prossima legislatura per nessuna votazione popolare siano chiamati a partecipare a prove pilota del voto elettronico aventi luogo contemporaneamente più del 10 per cento degli aventi diritto di voto. Inoltre, in caso

¹⁰⁵ FF 2002 596

di referendum obbligatori, per i quali è determinante anche la maggioranza dei Cantoni, non sarà ammesso al voto elettronico più del 20 per cento dei corpi elettorali cantonali interessati.

Il voto elettronico è un sistema complesso con numerosi partecipanti a molti livelli diversi. La sua introduzione a tappe consente di raccogliere esperienze e di integrarle nel perfezionamento del voto elettronico. Il voto elettronico potrà essere introdotto solo quando tutti i partecipanti – i cittadini, i politici e le autorità – si saranno abituati alle nuove modalità e strutture, le avranno assimilate e avranno fiducia in esse. È opportuno adottare una procedura prudente anche per contenere i rischi.

Il Consiglio federale ritiene ancora che sia necessaria una suddivisione in quattro tappe¹⁰⁶ (1. Possibilità di svolgere votazioni elettroniche. 2. Possibilità di svolgere elezioni elettroniche. 3. Possibilità di firmare elettronicamente referendum e iniziative e 4. proposte di candidature per le elezioni del Consiglio nazionale).

5.4.2 Necessità di adeguare le basi legali

Nell'ambito del voto elettronico sono necessari adeguamenti a livello sia di LDP, che di ODP.

A livello di legge deve essere tenuto conto dello stato attuale dei lavori in materia di voto elettronico ed essere resa possibile l'estensione controllata delle prove pilota. Inoltre devono essere create le basi per l'armonizzazione dei cataloghi elettorali quale condizione perché possano votare per via elettronica gli Svizzeri all'estero aventi diritto di voto.

- Completamento della LDP con un articolo 8a capoverso 1^{bis}: attualmente i Cantoni pilota devono chiedere un'autorizzazione per ogni votazione popolare federale e sottoporre la sperimentazione all'approvazione del Consiglio federale. In futuro il nostro Collegio dovrà essere abilitato a consentire ai Cantoni che avranno effettuato serie di test con esito positivo (almeno cinque sperimentazioni consecutive senza avarie per le votazioni popolari federali) di impiegare il voto elettronico per un certo periodo di tempo per votazioni popolari federali limitandolo sotto il profilo territoriale, temporale e materiale. Le condizioni e la durata delle prove ampliate saranno definite dal nostro Collegio che avrà anche la facoltà di limitare di nuovo o vietare in qualsiasi momento il voto elettronico. Questo dispositivo di emergenza si ispira a un meccanismo già utilizzato a più riprese per il voto per rappresentanza nei plebisciti sul Giura e sul distretto di Laufen (RU 1974 887 e 2215, 1975 1295, 1978 580, 1983 750, 1989 1780 e 1994 2424 n. II).
- Abrogazione dell'articolo 8a capoverso 3: per la fase sperimentale ampliata, non è più necessario il severo obbligo della consulenza scientifica, che può pertanto essere stralciato, soprattutto per considerazioni di ordine finanziario. Se necessario, il nostro Collegio potrà far rilevare ulteriori dati sull'impiego del voto elettronico e prevedere la consulenza scientifica nell'ambito della sua competenza di disciplinare i dettagli (art. 8a cpv. 4 LDP). La consulenza scientifica rimane comunque possibile anche se la leg-

¹⁰⁶ Ibidem, pag. 596

ge non la prevede in modo esplicito. A tempo debito, il Consiglio federale informerà l'Assemblea federale sui risultati della sperimentazione ampliata.

- Completamento della legge federale sui diritti politici degli Svizzeri all'estero (LDPSE, RS 161.5) con un articolo 5b (nuovo): i Cantoni in cui gli Svizzeri all'estero non hanno diritto di voto a livello comunale stabiliscono se il catalogo elettorale per gli Svizzeri all'estero è tenuto centralmente dall'amministrazione cantonale o dall'amministrazione della capitale cantonale. I cataloghi elettorali degli Svizzeri all'estero possono essere gestiti in modo decentralizzato a condizione che siano armonizzati a livello cantonale e gestiti elettronicamente o a condizione che i dati siano trasmessi regolarmente per via elettronica a un catalogo elettorale degli Svizzeri all'estero gestito centralmente.

Queste modifiche di legge sono state sottoposte nel messaggio del 31 maggio 2006 sulla riforma dei diritti politici¹⁰⁷. Inoltre prevediamo di integrare a livello di ordinanza le conoscenze acquisite nell'ambito dei progetti pilota e dello scambio internazionale di esperienze e di comunicarle a tutti i Cantoni.

5.4.3 Misure di accompagnamento di politica sociale

In caso di introduzione del voto elettronico in Svizzera, si corre il rischio, piccolo ma reale, che si accentui ulteriormente la differente partecipazione a votazioni ed elezioni per sesso e gruppi di età.

In altre parole, il voto elettronico potrebbe aumentare leggermente nell'ambito politico¹⁰⁸ il divario digitale che si registra in molti settori della vita. Secondo un rapporto della Scuola universitaria professionale di tecnica, economia e lavoro sociale di San Gallo (Fachhochschule für Technik, Wirtschaft und Soziale Arbeit) vi sono, in caso di introduzione del voto elettronico, due misure di accompagnamento¹⁰⁹ per evitare di correre questo rischio:

- *usabilità*: la progettazione e la configurazione del voto elettronico sono conformi alle esigenze delle persone che hanno poche conoscenze del computer. A tal fine occorrono strutture di navigazione chiare, percorsi di navigazione brevi, un linguaggio semplice e dimensioni e colori dei caratteri facilmente

¹⁰⁷ Messaggio concernente l'introduzione dell'iniziativa popolare generica e la revisione della legislazione sui diritti politici del 31 maggio 2006 (FF 2006 4815). Per quanto riguarda lo stato delle basi giuridiche cantonali per il voto elettronico cfr. la documentazione complementare 2.

¹⁰⁸ Per la problematica del divario digitale, cfr. Ufficio federale della formazione professionale e della tecnologia, Divario digitale in Svizzera (Digitale Spaltung in der Schweiz), rapporto all'attenzione del Consiglio federale, Berna 2004, www.isps.ch/site/attachdb/show.asp?id_attach=943; come pure Vodoz Luc et al., Ordinateur et précarité au quotidien: les logiques d'intégration provisoire de la formation continue (Computer e precarietà nella vita quotidiana: le logiche dell'integrazione provvisoria della formazione continua), Rapporto finale del progetto «Il divario digitale: emergenza, evoluzione, sfide e prospettive» elaborato nell'ambito del Programma nazionale di ricerca PNR51 «Integrazione e esclusione», Losanna 2005, <http://ceat.epfl.ch/docs/457.pdf>.

¹⁰⁹ Cfr. Ingold S., E-Voting: Welche Massnahmen sollen getroffen werden, damit E-Voting auch für Frauen attraktiv ist? (Voto elettronico: quali misure adottare per renderlo interessante anche per le donne?) Rapporto con raccomandazioni realizzato su incarico del «gruppo di lavoro gender mainstreaming» della Confederazione, luglio 2005 (cfr. la documentazione complementare 11e).

leggibili. L'adozione di queste misure è necessaria anche per altri motivi: l'articolo 14 capoverso 2 della legge federale del 13 dicembre 2002 sull'eliminazione di svantaggi nei confronti dei disabili (Legge sui disabili, LDis, RS 151.3) prescrive che «nella misura in cui le autorità offrano le loro prestazioni su Internet, tali prestazioni devono essere accessibili senza difficoltà alle persone ipoventi». I Cantoni devono applicare le disposizioni della LDis in caso di introduzione del voto elettronico. La collaborazione con le organizzazioni dei disabili può rivelarsi fruttuosa;

- *informazione della popolazione*: in caso di introduzione del voto elettronico, la Confederazione, i Cantoni e i Comuni potrebbero sensibilizzare i futuri cittadini alla tematica del voto elettronico nell'ambito dell'insegnamento dell'educazione civica. Manifestazioni informative e corsi per persone di ogni età e di ambo i sessi potrebbero contribuire a prevenire eventuali effetti negativi del voto elettronico sulla sovra o sotto rappresentanza a livello di partecipazione politica.

5.4.4 Organizzazione del seguito dei lavori

I sistemi di voto elettronico sinora impiegati con successo potranno essere utilizzati anche nella prossima legislatura alle condizioni descritte ai numeri 5.4.1 e 5.4.2. I Cantoni interessati possono aggregarsi a un progetto pilota oppure realizzare uno sviluppo proprio. La Cancelleria federale segue i progetti secondo il modello affermato nella fase pilota. La condizione è il mantenimento da parte del nostro Collegio delle esigenze definite nell'articolo 27a segg. ODP per i sistemi di voto elettronico e di un centro di competenze per la loro verifica. Un centro di competenze presso la Confederazione origina spese dell'ordine di 350 000 franchi all'anno in caso di introduzione graduale del voto elettronico. In questi costi fissi sono compresi i costi di personale per i compiti di coordinamento e il monitoraggio di progetti cantonali (2 posti di collaboratori scientifici) e i costi di materiale per controlli tecnici esterni della sicurezza dei sistemi utilizzati, stimati a 100 000 franchi all'anno.

6 Considerazione conclusiva

I progetti pilota hanno permesso di valutare la fattibilità, le opportunità e i rischi del voto elettronico e hanno mostrato che il voto elettronico è fattibile, ma anche che è necessario porre e mantenere sotto controllo rischi in continua evoluzione. Le conoscenze e i metodi degli hacker mutano; per questo motivo, le misure di sicurezza non possono essere sviluppate definitivamente, ma vanno adeguate costantemente ai rischi.

Per realizzare il voto elettronico, avevamo proposto una suddivisione in tappe, basata sulla complessità delle singole problematiche, già nel rapporto del 9 gennaio 2002 (FF 2002 596 segg., 610 e 614 seg.). Ora occorre definire più dettagliatamente questo approccio. In un primo passo si devono armonizzare i cataloghi elettorali cantonali secondo standard federali; successivamente si deve realizzare il voto elettronico per le votazioni popolari e, nella tappa seguente, per le elezioni del Consiglio nazionale; solo nell'ultima tappa, essendo l'operazione più complessa,

seguirà la firma per via elettronica di domande di referendum e iniziative popolari federali come pure di proposte di candidatura.

L'obiettivo resta quello di consentire alle generazioni future la partecipazione democratica anche se cambiano le condizioni di vita; in altre parole, di assicurare la partecipazione in una forma conforme alle nuove abitudini di vita. Si deve raggiungere l'obiettivo senza mettere in pericolo le votazioni federali. In questo ambito, la sicurezza è più importante della velocità.

La prima tappa deve essere suddivisa in sequenze adeguate. Per la strutturazione del progetto svolgono un ruolo decisivo il contesto federalista e il valore aggiunto che può essere conseguito nelle singole sequenze.

Il valore aggiunto del voto elettronico è massimo per gli Svizzeri all'estero. Un voto elettronico per questo segmento di aventi diritto di voto presuppone l'armonizzazione a livello cantonale del catalogo elettorale specifico per Svizzeri all'estero. Solo così l'infrastruttura e le conoscenze specialistiche di alta tecnologia possono raggiungere la massa critica che consente di offrire il voto elettronico agli Svizzeri all'estero a un prezzo accettabile. Con messaggio del 31 maggio 2006 proponiamo che i Cantoni che non prevedono il diritto di voto comunale per gli Svizzeri all'estero concentrino il catalogo degli Svizzeri all'estero, a loro scelta, presso l'amministrazione cantonale o presso l'amministrazione della capitale cantonale. Le risorse e l'infrastruttura per un'offerta funzionale a tutti gli Svizzeri all'estero interessati aventi diritto di voto sono più facili da mettere a disposizione da parte di due dozzine di centri che non da oltre 2800 Comuni per lo più con pochi abitanti. Una centralizzazione a livello di Confederazione, invece, porterebbe solo perdite in termini di efficienza e ritardi perché sia la maggioranza dei Cantoni (art. 142 cpv. 2 e 3 Cost.) per due terzi delle votazioni popolari sia i circondari elettorali (art. 149 cpv. 3 Cost.) per l'elezione del Consiglio nazionale richiedono comunque che i risultati delle votazioni siano determinati separatamente per Cantone.

Non è il caso né di rinunciare a continuare le prove pilota in materia di voto elettronico né di estenderle con fretta eccessiva. Se restano inutilizzati, il know how e la tecnologia invecchiano rapidamente e perdono tutto il loro valore a causa del rapido progresso. Non si devono investire i soldi dei contribuenti per sviluppare sistemi, valutarne la fattibilità e abbandonarli dopo prove coronate da successo e poi sviluppare una seconda volta o acquistare all'estero il know how nel frattempo perso. L'obiettivo a lungo termine della semplificazione del voto e i diritti politici «cresciuti» organicamente dal basso nella struttura federalistica della Svizzera sono fattori determinanti anche per l'ulteriore sviluppo del voto elettronico.

Le prove iniziate con successo devono poter essere proseguite con la nostra autorizzazione. In futuro, il nostro Collegio dovrà essere abilitato a consentire ai Cantoni che avranno effettuato serie di test con esito positivo (almeno cinque sperimentazioni consecutive senza avarie per le votazioni popolari federali) di impiegare il voto elettronico per un certo periodo di tempo per votazioni popolari federali. Le condizioni e la durata delle prove ampliate saranno definite dal nostro Collegio che avrà anche la facoltà di limitare di nuovo o vietare in qualsiasi momento il voto elettronico. Nell'ambito delle autorizzazioni provvederemo a fare in modo che nel corso della prossima legislatura non siano chiamati a partecipare a prove pilota del voto elettronico aventi luogo contemporaneamente più del 10 per cento degli aventi diritto di voto a livello federale. Inoltre, in caso di referendum obbligatori, per i quali è determinante anche la maggioranza dei Cantoni, non sarà ammesso al voto elettro-

nico più del 20 per cento dei corpi elettorali cantonali interessati. In considerazione di tutte le circostanze potremo limitare in qualsiasi momento in modo più vasto il voto elettronico sotto il profilo territoriale, temporale e materiale, vincolarlo a condizioni o vietarlo.

Uno scenario del genere contiene il potenziale per un perfezionamento organico. Altri Cantoni interessati possono aderire a un sistema già realizzato o combinare adeguatamente elementi di diversi sistemi già impiegati con successo. In virtù delle convenzioni con la Confederazione, i Cantoni pilota forniscono, su basi non commerciali, ai Cantoni interessati il loro know how sviluppato con il contributo finanziario della Confederazione. Nuovi Cantoni interessati non ricevono più sussidi federali per il voto elettronico. Anche essi devono svolgere dapprima serie di prove; per le votazioni federali hanno bisogno della nostra autorizzazione e precisamente alle stesse condizioni come precedentemente i Cantoni pilota¹¹⁰.

Questo modo di procedere è basato su esperienze fatte precedentemente con la realizzazione di altre facilitazioni di voto (voto anticipato, urna itinerante, voto per rappresentanza e voto per corrispondenza), pure introdotte a tappe e in modo organico nei Cantoni. Offre il vantaggio che ogni Cantone può sviluppare il voto elettronico in sintonia con le sue strutture e abitudini e in modo conforme alle esigenze della sua popolazione. Come insegnano le esperienze fatte con altre forme di voto agevolato, la facilitazione di voto deve affermarsi sul mercato e questo mercato non deve in nessun caso evolvere allo stesso modo e alla stessa velocità e intensità in tutti i Cantoni.

Questo procedimento federalistico e prudente permette di risparmiare costi anche sotto un altro punto di vista: l'esperienza mostra che l'infrastruttura EED deve essere sostituita ogni quattro – sei anni. L'introduzione del voto elettronico in un Cantone o in molti Comuni non richiede in tal modo una sostituzione capillare, particolare o straordinaria dell'infrastruttura prima dell'ammortamento degli impianti esistenti.

In questo senso deve essere cancellato anche l'obbligo della consulenza scientifica per le prove pilota di voto elettronico. Nei casi in cui è razionale e fattibile con un onere ragionevole, potremo ordinare anche in futuro simili rilevamenti; ma non vi saremo più tenuti indipendentemente dall'ammontare dei costi.

Il Cantone che vuole invece impiegare il voto elettronico per votazioni federali concernenti iniziative popolari con controprogetto o elezioni del Consiglio nazionale ha bisogno di svolgere prima le corrispondenti sperimentazioni e dell'autorizzazione del nostro Collegio. In questo ambito si applicano le stesse regole come precedentemente per le prime prove di voto elettronico in occasione di votazioni popolari federali.

¹¹⁰ Cfr. la nostra Circolare del 20 settembre 2002 ai Governi cantonali concernente la revisione parziale dell'ordinanza sui diritti politici [condizioni di autorizzazione per lo svolgimento di prove pilota cantonali del voto elettronico], FF 2002 5891.

Glossario tecnico

| | |
|---------------------------------|---|
| Autenticità | = Proprietà di una persona, di un messaggio o di un processo di essere identico, in modo verificabile, a una persona, un messaggio o un processo noto da altre fonti. |
| Cavallo di Troia | = Programma indipendente con una funzione devastatrice nascosta. Nel sistema operativo di un sistema riesce spesso a diffondersi indisturbato, a procurare ad altri l'accesso al server attraverso una porta secondaria, distruggere dati importanti o a scoprire password. |
| Challenge-Response (procedura) | = Procedura di autenticazione. Il sistema di destinazione emette una parola generata casualmente (challenge). L'utente che desidera autenticarsi nei confronti del sistema di destinazione risponde con una «response» adeguata. La procedura è molto più sofisticata dell'impiego delle tradizionali parole d'ordine. |
| Code-Voting | = Le caratteristiche di voto non sono indicate sul canale di trasmissione con «si», «no», «scheda bianca», ma con un codice alfanumerico (ad es. «Az7k9» per «si»). Vi sono due varianti di code-voting: l'avente diritto di voto immette il codice direttamente nei campi previsti oppure un simile codice è generato automaticamente in background. |
| Domain Name Server (DNS) | = Server che traduce gli indirizzi testuali in indirizzi numerici (indirizzi IP) (p. es. www.beispiel.biz = 130.92.63.17) |
| File di log | = File con il quale può essere registrato ad esempio l'uso di un sito. I file di log sono la base per valutare l'efficienza e il rendimento di un sito web. |
| Fingerprint (impronta digitale) | = Somma di controllo di certificati. Ogni certificato dispone di un fingerprint univoco per cui è facile appurare mediante verifica se si è collegati con il server desiderato. |
| Firewall | = Inglese per «barriera di protezione contro il fuoco»: hardware o software che controlla e protegge il flusso dei dati contro accessi non autorizzati tra due o più reti. |
| Hacker | = Per hacker si intendono persone che si introducono in computer per spiare dati. Spesso i termini «hacker» e «cracker» sono utilizzati erroneamente come sinonimi. La differenza risiede nell'energia criminale: gli hacker sono animati da «spirito sportivo» e non provocano danni durevoli. I cracker invece non si limitano a spiare i dati, ma li falsificano, rubano, cancellano o rendono inutilizzabili. |
| Man-in-the-middle (attacco) | = Alice vuole inviare a Bob un messaggio con la posta elettronica. Durante la trasmissione Carlo intercetta il messaggio, lo cambia e lo inoltra a Bob, che non si accorge del cambiamento se il messaggio non era criptato. |
| Metodo open source | = Metodo in base al quale il codice sorgente di un software è reso pubblico. |

| | |
|---------------------------|---|
| Provider | = Ditte e organizzazioni che – attraverso un server proprio – forniscono servizi specifici a Internet come l’accesso, progetti globali di presentazione, spazi di memoria per pagine web ecc. |
| Ridondanza | = Presenza di sistemi uguali o simili dal punto di vista funzionale. Grazie alla struttura ridondante dei sistemi aumentano considerevolmente la sicurezza d’esercizio e la sicurezza contro i guasti. |
| Secure Socket Layer (SSL) | = Pagine internet certificate. I dati immessi in queste pagine sono criptati e possono essere decriptati solo dal destinatario abilitato. È una procedura standard praticata ad esempio nell’e-banking. |
| Spoofing | = «manipolare» o «artefare». Hacker falsificano un indirizzo in Internet per convogliare ad es. dati verso un elaboratore falso. Terzi potrebbero così leggere lo scambio di dati esterno. Protocolli di criptaggio possono costituire un rimedio efficace. |
| Usabilità | = Facilità d’uso |

Fonti delle definizioni

Wikipedia, l’enciclopedia libera consultabile on line: www.wikipedia.org/.

Documentazione complementare

Informazioni complementari in forma elettronica sui seguenti temi sono pubblicate in una documentazione separata:

1. Bibliografia e letteratura sull'argomento
2. Basi giuridiche per il voto elettronico nei Cantoni
3. Basi giuridiche per la gestione del catalogo elettorale nei Cantoni
4. Quadro sinottico delle prove pilota negli anni 2003–2006
5. Valutazione dei sistemi cantonali in base alle esigenze legali minime stabilite negli articoli 27a–q ODP per progetti pilota del voto elettronico
6. Quadro sinottico delle misure di sicurezza realizzate nell'ambito dei progetti pilota cantonali
7. Tabella riassuntiva dei costi dei progetti pilota cantonali
8. Sondaggio 2005 presso i Cantoni e i Comuni sul voto per corrispondenza, Berna 2005
9. Voto elettronico e voto per corrispondenza. Problemi di sicurezza e misure
10. Quadro sinottico di prove pilota di voto elettronico all'estero
11. Studi esterni (ricerca parallela)
 - a. Istituto di ricerca gfs.bern, Das Potenzial der elektronischen Stimmabgabe, studio redatto su incarico della Cancelleria federale, Berna 2005
 - b. Centre d'études et de documentation sur la démocratie directe de l'Université de Genève, Analyse du scrutin du 26 septembre 2004 dans quatre communes genevoises (Anières, Carouge, Cologny e Meyrin), luglio 2005
 - c. Canton de Neuchâtel, Enquête de satisfaction, scrutin du 25 septembre 2005, novembre 2005
 - d. Centre d'études et de documentation sur la démocratie directe de l'Université de Genève, Umfrage bei Stimmberechtigten der Zürcher Gemeinden Bertschikon, Bülach und Schlieren anlässlich des Pilotversuchs zum Vote électronique vom 27. November 2005, febbraio 2006
 - e. Ingold S., E-Voting: Welche Massnahmen sollen getroffen werden, damit E-Voting auch für Frauen attraktiv ist? Rapporto con raccomandazioni realizzato su incarico del «gruppo di lavoro gender mainstreaming» della Confederazione, luglio 2005

Questi documenti possono essere ordinati presso la Sezione dei diritti politici della Cancelleria federale oppure essere consultati e scaricati via Internet dall'indirizzo www.admin.ch (rubrica «Cancelleria federale/Sezione dei diritti politici/Voto elettronico»).

