Voto elettronico via **Internet** **(i.voting)** oppure **al Seggio** **(e.voting)** e con l'opzione **carta e matita**

mantenedo e migliorando le funzionalità dei Seggi (nell'i.voting molto ridotti in numero)

mantenendo la possibilità di dare le "preferenze" (oggi non in uso)

e senza escludere l'eliminazione dei Seggi se l'esperienza ne evidenziasse la possibilità

9.8.2022 Bozza d'analisi, da verificare-completare con informatici pratici di Internet, token, smartphone etc…

in rosso i punti critici o da verificare

http://digilander.libero.it/gino333/00.procedura.docx http://digilander.libero.it/gino333/00.procedura.pdf

Prima di pensare all'informatica, conviene fare una **seria riflessione organizzativa** così come era buona abitudine nel secolo scorso quando le risorse informatiche erano assai modeste rispetto ad oggi. Per il voto internettiano vengono proposti sistemi centralizzati senza Seggi che costerebbero poco (come gestione), ma non convincono perché gli elettori si troverebbero di fronte a un "moloch" di cui occorre fidarsi ad occhi chiusi mentre i partiti verrebbero privati del controllo diretto e locale a cui hanno diritto. Invece col metodo qui proposto i **Seggi vengono mantenuti** ma, a regime, si può pensarli di ridurli **dagli attuali 60 mila a 10 mila,** uno per Comune o circoscrizione (comunque un bel risparmio). In ogni caso il voto manuale deve essere mantenuto a lungo per la **necessaria gradualità di introduzione** ed anche come una garanzia a fronte di qualsiasi imprevisto si presentasse. Mantenendo i Seggi si minimizzano i rischi perché **le uova non sono tutte nello stesso paniere** e se qualche Seggio fosse stato attaccato, la votazione si può rifare solo in quel Seggo (magari con carta e matita). Certo devono essere casi marginali: non si può pensare di dover votare e rivotare 10 volte prima che capiti una votazione esente da pasticci.

Opinione di uno **scettico**: "*Il voto elettronico è un problema ancora insoluto, in particolare per quel che riguarda elezioni delicate come quelle politiche nazionali in cui sia la criminalità organizzata sia diverse potenze straniere potrebbero avere interesse a manipolare i risultati. Tutto si riassume nel non avere, ad oggi, alcun metodo sicuro che garantisca l'impossibilità di modificare i dati senza lasciare traccia. Mettersi al riparo da un presidente di seggio curioso non è affatto sufficiente quando si ha a che fare con servizi segreti e affini. Infatti non basta assicurarsi che nessuno possa accedere ai dati contenuti nella macchina, ma che essa stessa non li modifichi di nascosto perché qualcuno l'ha programmata così. Già qui diventa difficile: come ci si assicura che il codice sorgente del programma di voto corrisponda davvero al codice binario caricato nella macchina? Come ci si assicura che il compilatore non sia stato modificato per introdurre una routine segreta? Come ci si assicura che lo stesso sistema operativo sia pulito? Come ci si assicura che i diversi microcode della macchina siano tutti puliti, in particolare quelli della CPU e dei supporti di memorizzazione? Il solo kernel di Linux (senza contare tutto il necessario contorno) conta ben 27 milioni di righe di codice e il relativo compilatore GCC almeno altri 5 milioni. Per non parlare delle specifiche dei microcode che spesso sono anche segreti industriali. Insomma, un pozzo senza fondo di problemi. Tutto questo senza poi contare i problemi legati alla trasmissione e conservazione dei dati: ogni passaggio potrebbe introdurre delle variazioni e se anche si stampasse un tabulato dei voti sarebbe poi difficile assicurarsi che il dato su carta corrisponda davvero a quello memorizzato*."

Terrificante, ma sono **problemi in buona parte evitabili.** Primo perché un conto è manomettere un server un altro manometterne 10 mila. Secondo perché l'elettore potrà **controllare la presenza del proprio voto nell'urna** perciò ogni imbroglio verrà scoperto e l'imbroglione perderà la faccia, quindi potenze straniere e partiti non avranno convenienza nel tentare di alterare i dati**.** Certamente ciò **facilita il voto di scambio,** ma questo è sempre esistito e oggi basta un telefonino per fotografare la scheda unitamente a qualcosa fornito dal compratore del voto. Vero che è vietato portare telefonini nel Seggio, ma **nessuno oggi perquisisce chi va a votare, neanche a campione**. Anche la Svizzera prevede che l'elettore possa verificare la presenza del proprio voto: *https://www.evoting.ch/it "... procedura ... di verificabilità individuale. In questo modo gli elettori possono verificare se il loro voto è stato trasmesso senza variazioni e se è stato registrato correttamente all'interno dell'urna elettronica ... "* quindi per loro il controllo della regolarità delle operazioni e la fiducia che il cittadino deve avere nel sistema è più importante del possibile voto di scambio.

Non mi è noto il metodo che intendono usare, qui proporrò semplicemente l'aggiunta al voto di una frase a piacer dell'elettore. Anche senza questa opzione, col voto internettiano si può vendere il voto andando a votare in casa dell'acquirente, ma lo stesso succede col voto postale (nelle NOTE altre considerazioni). Capisco l'importanza dei principi costituzionali (per la verità piuttosto disattesi) ma ha poco senso preoccuparsi del voto di scambio se non c'è modo d'impedirlo, ad impossibilia nemo tenetur. Oltre ai telefonini, oggi è certamente possibile fabbricare dispositivi grandi come un'unghia capaci di fare una foto e poi visualizzarla in un dispositivo posseduto da chi ti ha comprato il voto. Dobbiamo denudare l'elettore per vedere se ce l'ha? Non è meglio tener conto della realtà dei fatti e beneficiare dei vantaggi del voto elettronico? Si consideri poi che la possibilità di controllare il proprio voto è fondamentale per creare nella gente la richiesta fiducia nel sistema.

A parte le potenze straniere e i partiti (stoppabili come detto) resta però il **pericolo degli hacker** che volessero divertirsi a **far casino solo per il gusto di farlo**. Bisogna cioè impedire che qualcuno possa entrare in qualche server di Seggio e pasticciare o distruggere i dati. Mi è stato detto che **"con un firewall basato su FreeBSD e con uno Snort come IDS/IPS nessuno può entrare":** per ora lo assumo per vero, ma aspetto conferma.

Segretezza del voto nessun sistema oggi può garantirla al 100%. Si vedrà che la procedura fornisce di per sé ottime garanzie perché al momento del voto l'identificativo del votante e il voto transitano in tempi diversi mentre l'identificativo si collega al nome del votante tramite **molteplici file non presenti nei Seggi** e non raggiungibili via Internet quindi reperibili da terzi solo corrompendo i gestori (punto molto importante che richiede specifica analisi). Pertanto il collegamento fra voto e nome del votante sarà molto difficoltoso, quindi non sembrano necessarie specifiche criptature oltre al normale SSL/TLS. Inoltre chi non si fida e vuole le **stesse garanzie attuali, potrà votare con la**

carta e la matita. In questo senso la sicurezza è garantita. Alla fine, se l'esperienza dimostrasse non ci sono interferenze o che sono tollerabili o che novità tecnologiche risolvono di per sé ogni problema, allora i Seggi potranno essere del tutto eliminati.

Poi **le urne elettroniche e le relative totalizzazioni** (di ogni Seggio) **dovranno essere messe a disposizione di tutti** affinché, oltre al controllo della presenza del proprio voto, tutti possano rifare le totalizzazioni con programmi propri: sarà quindi impossibile che un servizio segreto possa di alterare i dati o il microcodice di tutti i compiuterini del mondo. **La disponibilità e la chiarezza dei dati supererà ogni problema di "sistema proprietario" o di "open source".** Se sono garantiti i dati, se i dati sono a disposizione di tutti e se tutti possono rifare tutti i conteggi con software personale, **non è indispensabile "garantire" il software** (che però dev'essere abbastanza sicuro per evitare di ritrovarsi poi con risultati da gettare).

Ed ancora, per **ridurre** (di molto) la possibilità di **interferenze** e per **comodità del votante** il **voto sarà in due fasi**:

1) alcuni giorni vanno concessi all'elettore per allacciarsi ad un SITO NAZIONALE per visualizzare il tabellone del proprio seggio ed effettuare le scelte di voto che verranno poi memorizzate su di un supporto personale (magari una chiavetta per le prime fasi di test). Questa fase potrà godere dei più potenti ausili grafici disponibili (ormai la gente è viziata), ma si dovrà dare all'elettore la possibilità di verificare la correttezza del voto trascritto nel proprio supporto in modo che possa poi spedirlo senza porsi dubbi (se non fosse corretto potrà rigeneralo o caricarlo a mano). Poiché in questa fase non è necessario inviare l'identificativo del votante, un eventuale intruso non potrà abbinare il voto al votante. Nell'ipotesi che l'indirizzo fisico della macchina usata dall'elettore possa essere visto da terzi, chi non volesse assolutamente far sapere le sue intenzioni di voto (fortunatamente sempre di meno al giorno d'oggi) può usare un mezzo di uso pubblico (questo anche nella successiva fase di consegna del voto), oppure può eseguire più scelte in modo non si sappia quale scelta verrà poi spedita). Se poi le alternative di voto fossero modeste, il voto potrebbe essere annotato a mano (si veda dopo). In questa prima fase il voto non viene registrato nell'urna elettronica, ma "consegnato" all'elettore il quale

2) avrà **un giorno (o qualche ora)** per spedire il voto al proprio seggio d'iscrizione. In questa la fase il software sarà **semplificato al massimo** in modo che i rappresentanti di lista possano **toccare con mano** lo svolgersi delle operazioni (naturalmente assisti da un tecnico informatico comunale). Il server del seggio dovrebbe essere dotato di un sistema operativo quanto più inattaccabile possibile (nelle NOTE finali si vedano considerazioni sull'uso di Linux) e magari ridotto alle sole operazioni da compiere (sinteticamente: verificare se l'elettore appartiene al seggio, se ha l'età per quel voto, se non ha già votato e infine registrare il voto segnalando che l'ha fatto). Si noti che in questa fase transita nella memoria di calcolo un identificativo dell'utente, ma non il nome dell'utente. Nel file dei voti non è presente l'identificativo (consentirebbe di risalire al nome avendo accesso a specifici archivi anagrafici che però non devono essere presenti nel Seggio cosa che rende più difficile abbinare voto e votante). Importante considerare che poiché i controlli di validità del voto sono demandati alla fase 1 (di cui qui non ci occupiamo), **il software dei server dei seggi non avranno bisogno di aggiornamenti**, neppure per quelli legati alle particolarità del voto e ciò **semplificherà enormemente la gestione del sistema.**

> Le funzioni di un server di seggio così limitato nelle sue funzioni riduce i rischi e magari potrebbe (in seguito) giustificare la redazione di un **sistema operativo mirato per questi semplici compiti** (cosa che renderebbe ancor più difficile l'attività di hacker malevoli): per chi fosse pratico del mondo IBM del secolo scorso, si immagini una specie di SSP con le OCL usate per comunicare col votante e con l'aggiunta di quello che richiede Internet. In ogni caso il sistema operativo del server di seggio e il suo software, una volta dimostrato che operano con successo non richiederanno d'essere aggiornati per decenni (salvo stravolgimenti nelle procedure elettorali o l'arrivo di miglioramenti tecnici attraenti) e quindi non ci si sarà da preoccuparsi per manipolazioni future (è negli aggiornamenti che si corrono i maggiori rischi).

Anche l'hardware può essere mantenuto per tempi lunghi: **se funziona oggi perché non potrà funzionare domani**? Che importa che sia "vecchio"? Basta che faccia il suo mestiere! Naturalmente salvo stravolgimenti nella rete. I server di Seggio non dovrebbero assolutamente essere usati per altri scopi e fra un'elezione e l'altra andrebbero tenuti chiusi a chiave ed essere raggiungibili solo in presenza dei rappresentanti di tutti i partiti, a meno che prima dell'uso il server non venga ripulito di tutto e il suo software non venga ricaricato con supporti forniti da uno specifico ufficio gestito dall'insieme dei partiti.

In ogni Seggio, al termine delle procedure di voto, **le urne digitali verranno salvate in tante copie e consegnate ad ogni partito e in seguito pure ad ogni cittadino che le volesse avere**: se gli archivi rispettassero le modalità del secolo scorso potrebbero richiedere circa un MB per ogni Seggio (quanto una fotografia poco dettagliata) quindi:

- grazie alle copie delle urne digitali tutti potranno controllare i totali di seggio dichiarati dai rappresentanti di lista del seggio
- tutti potranno accedere ai totali dichiarati dai vari seggi e poi controllare le totalizzazioni a qualsiasi livello Per comodità i dati verranno certamente tenuti anche in linea, ma chiunque possiede una copia originale potrà confrontarla con ciò che si trova in linea e segnalare ogni alterazione a posteriori. **Partiti e servizi segreti si stuferanno subito nel tentare inutili contraffazioni**, magari gli hacker no; in tal caso, se sopravvenissero dubbi, si useranno le copie originarie rielaborate in organizzazioni pubbliche e interpartitiche.

Inoltre i rappresentanti di lista potranno testare il sistema durante le votazioni con votazioni fasulle evidenziando subito eventuali interferenze (vedi avanti Passo E),

La metodologia proposta potrà essere usata anche per il voto elettronico al seggio **(e.voting) e questo senza problemi di segretezza** consentendo conteggi rapidissimi e controllabili da tutti (ma lo terrei di riserva nel caso si dimostrasse che viaggiare in Internet è troppo pericoloso).

Certamente la legge dovrà autorizzare il voto elettronico, ma la cosa è facilitata dal fatto che il sistema proposto ricalca la struttura attuale consentendo una sperimentazione sotto il controllo dei partiti e quindi priva di rischi che possano sfuggire al controllo. Basterebbe un "ok provate pure" (non ha senso un regolamento minuzioso di qualcosa ancora sperimentale). Si può cominciare anche con un sol seggio in tutta Italia e vedere che succede (questo al costo di poche migliaia di euro, tutto compreso). I seggi sono attualmente 60.000 ma, come detto, col voto internettiano (i.voting) man mano che gli elettori opteranno per il voto elettronico, si può pensare di scendere a circa 10.000 (un seggio per Comune o Circoscrizione). Per evitare l'acquisto di server poi inutilizzati si può procedere per zone in modo che le macchine in eccesso in una zona possano essere dirottate in un nuova zona.

Per un primissimo test sul campo converrebbe trovare un Comune desideroso di consultare i cittadini in merito alle decisioni locali: potrebbe cavarsela con poche migliaia di euro. Dopo la verifica, correzione e approvazione dell'analisi, i passi potrebbero essere i seguenti:

- *si scrive il software per digitalizzare il seggio (basta la parte per l'e.voting)*
- *lo si testa grazie alla collaborazione di alcuni dipendenti comunali (basta un sol seggio).*
- *se ok si scrive il software per votare via Internet (i.voting e lo si prova coi dipendenti comunali)*
- *se ok si fa il software di riepilogo dei seggi e si fa un test con paio di seggi*
- *se ok si istituisce il premio per gli hacker (vedi dopo) che riuscissero a scassinare il sistema*
- *se ok il Comune completa la propria struttura e comincia ad usarla (mantenendo il premio hacker).*

Quindi qualcosa di semplice, comprensibile per molti, dove sarebbe la sorveglianza dei rappresentanti di lista e dei singoli cittadini a garantire la correttezza delle operazioni, non enti di certificazione, blockchain e diavolerie varie, cose che lasciano certamente perplessi la stragrande maggioranza dei cittadini. Naturalmente non basta essere in grado di riconoscere eventuali manipolazioni, bisogna anche che queste possano accadere di rado): questo dev'essere assicurato dalla procedura e confermato dai primi utilizzi, ben certi però che la perfezione 100% non esiste in nessuna cosa umana (chi la pretendesse vuol dire che ha interessi opposti).

Nelle prime prove si può usare come server un normale PC con un normale sistema operativo (che nell'e.voting andrà bene sempre) e come strumento di voto un altro PC + un semplice token USB (https://www.gochange.it/business/token-sicurezza-chiavetta-usb/4350 chiedere ad esperti possibilità operative attuali). Solo se i risultati fossero incoraggianti converrà migliorare lo strumento di voto magari derivandolo dall'home banking integrato con l'invio dell'impronta digitale o col "riconoscimento facciale" (addirittura si potrebbe pensare anche a una specie di telefonino personalizzato e ridotto al solo uso del voto che il Comune potrebbe omaggiare ad ogni nuovo elettore). NB maggio 2022 vidi https://www.telefonino.net/notizie/android-password-fido-supporto/ eviterebbe l'uso di password. Quanto ai pericoli di Internet, pare che a suo tempo Obama avesse pensato ad una specie di rete parallela più sicura per gli usi delicati: se non è un ricordo distorto o fallito varrebbe la pena di sollecitare chi di dovere ☺. Invece per le elaborazioni di seggio successive alle operazioni di voto converrà usare un normalissimo PC **non** in rete.

I guasti tecnici sembrano improbabili e produrrebbero danni limitati (vista la frammentazione dei server di voto) ma non sarebbe un problema rifare la sola fase di voto digitale dei seggi che avessero avuto problemi (e se il problema fosse irrisolvibile si potrebbe rivotare con carta e matita). L'eventuale ripetizione di voto potrebbe essere condizionata alla richiesta di almeno uno dei partiti considerando che la cosa non avrebbero senso se i risultati non potessero essere ribaltati.

Serve naturalmente una **Comitato Interpartitico Elettorale** (a cui faranno riferimento i rappresentanti di lista e gli addetti informatici dipendenti dal Comune o assunti per l'occasione) col compito di sovrintendere, di fornire e garantire il (ridottissimo) software necessario e di raccogliere i dati. **Gestirà pure** (a piacer suo) **il sistema centralizzato** per la **fase 1)** quella in cui si prepara il voto da spedire. Altre strutture statali (provincie e ministero dell'interno) non sono indispensabili, ma non guastano. Presso il Comitato si collocherà un server di seggio (utile per testare le attività in corso come al Passo E), da usare anche per il **premio per gli hacker**: vi si potrebbe immettere un record in uno specifico file (che non dovrà essere aperto da nessuno fino al termine del Passo 11) contenente una stringa (ad es. xyz19+2apq…) composta con caratteri immessi dalle varie liste l'una all'insaputa delle altre. Chi la comunicasse prima della fine del Passo 11 riceverà il premio, doppio se aggiungesse un seconda stringa (e allora i gestori del sistema avrebbero di che preoccuparsi). Qualcosa di simile si può pensare anche presso i singoli Seggi.

METODO PROPOSTO, alcuni dettagli informatici:

si è già detto che per la preparazione del voto ci si aggancia ad un unico sito centrale prevedendo l'utilizzo dei moderni sistemi di interfacciamento e di controllo della congruenza del voto (l'utenza è oggi abituata a cliccare sulle immagini). Ovviamente la scelta viene registrata a mezzo di *codici* cioè coi simboli usati al posto di parole soggette ad errori di scrittura o ambiguità, ad es.: **23** invece di Paolo Rossi. Oggi i codici in genere non si vedono, **basta "cliccare".** Invece in questa procedura conviene mantenere **la possibilità** di **immettere il voto anche scrivendo i codici,** questo anche perché possono esserci casi in cui la cosa è talmente semplice che non ha senso passare attraverso i disegnini di un programma dove qualcuno può aver messo errori o magari dei veri e propri imbrogli elettorali (e oggi, mancando le "preferenze" a mio parere siamo in questa situazione). "Cliccare" equivale a "mettere una croce": semplifica e consente di far votare anche chi non sa, o non sa più scrivere (magari proprio a causa dei computer ☺), ma la conoscenza dei codici sottostanti, oltre a bypassare il sistema centrale, permette anche di controllare facilmente se le proprie scelte sono state correttamente recepite dal sistema centralizzato (quindi il supporto dove verrà annotata la stringa di voto dovrà essere facilmente osservabile dal votante).

Per ulteriori garanzie di anonimato converrà tenere separato il sistema elettorale da ogni altro sistema, (anche dalla carta di identità digitale perché è meglio evitare eventuali problemi o aggiornamenti causati da altri enti). Come oggi

l'Anagrafe Comunale (o qualsiasi ente adibito a tale funzione) gestirà un file anagrafico con gli iscritti ad ogni seggio dove comparirà il **codice** di aggancio al **Token USB** (chiamiamolo **TK**) **o al dispositivo equivalente** assegnato ad ogni iscritto. Nel Token (o chi per lui) sarà stato inserito anche l'indirizzo **IP** (fisso) del seggio (o un identificativo del seggio nel caso dell'e.voting). Al decesso l'elettore verrà tolto dall'archivio (e quindi il suo token non potrà più essere utilizzato) idem se cambia residenza. Eventuali sistemi aggiuntivi di controllo (Pin, telefonata, impronte digitali, riconoscimento facciale …) sono lasciati ai successivi perfezionamenti del sistema identificativo).

Nel token (o altro), oltre al software necessario, dovrebbe essere disponibile spazio per annotare il voto che si intende esprimere (altrimenti servirà una seconda chiavetta USB e la procedura andrà modificata di conseguenza). L'anagrafe fornirà al seggio il file **FTK** (copiato dal file anagrafico, **ma senza il nome ed altri elementi identificativi** perciò chi riuscisse a mettere assieme TK e Voto dovrebbe poi poter accedere agli archivi anagrafici per violare la riservatezza (raddoppiandosi così le fatiche imposte agli hacker).

Supponiamo che il tabellone elettorale di seggio abbia questo aspetto:

---------- **Camera (<1)**----------				----------**Regione (<2)**----------		
PXX	**PZZ**	**IND**	(partiti)	**PXX**	**PZZ**	**PKK**
Mario (1)	**Sergio (4)**	**Ciccio (6)**		**Tizio (7)**	**Toni (9)**	**Mario (11)**
Piero (2)	**Rino (5)**			**Caio (8)**	**Caio Y (10)**	
Paolo (3)	vedi se la casistica è completa (nel caso estendere con criteri simili)					

Se non sono previste le preferenze le cose si semplificano, ma come si vede le preferenze sarebbero facilmente gestibili. I "codici" sono quelli fra parentesi, il carattere < sta per "scheda", i partiti non hanno codice perché lo sono già di per sé Nei codici saranno considerati sinonimi **< >** **1 I i ì !** **0 O o** **, . ; : - _ '** maiuscole equiparate alle minuscole.

Usando un telefonino per comunicare a mano si potrebbero usare solo i numeri, es: *1 *2 *3 (Camera Regione Senato …) **1 **2 **3 … (PXX PZZ IND …) ***11 ***2 ***10… (Mario di PXX, Piero, Caio Y …) e forse con l'uso di "cancelletto" si potrebbe ancor più semplificare (ormai siamo già stati abituati dai centralini telefonici ☹).

FILE possibilmente all'antica, cioè di lunghezza fissa con campi fissi, per semplicità e risparmio

FTK contiene tutti gli elettori del seggio **(senza nomi ed altri identificativi espliciti**)
TK codice del token (o altro) individuale (per violare la **riservatezza** bisogna abbinare TK all'anagrafica fuori linea)
Data di nascita (per sapere quali schede può votare e per usi statistici)
Comune di nascita, sesso, titolo di studio,… ? per usi statistici
Eseguito voto (1 byte , E= e-i.voting M=manuale) in bianco all'inizio.

FVOTI (conterrà le singole espressioni di voto dei cittadini, sia ai partiti, sia le eventuali preferenze)
Stringa di voto (un centinaio bytes)
Data di nascita, Comune di nascita, sesso, titolo di studio,…. ? per usi statistici (trascritti da FTK)
non contiene TK e quindi non agganciabile a TK in FTK e tantomeno all'identità anagrafica fuori linea.

FSINT (voto ai partiti)
Codice del Seggio …. es: Gruppo/Regione/Provincia/Comune/Quartiere/Seggio**…**
Scheda (2 bytes) (o quesito referendario etc….)
Sigla Partito (5 bytes?)
Voti Manuali (9 bytes) (bytes esagerati, nel caso che si arrivi ad un unico o a pochi seggi)
Voti Digitali (9 bytes) (se Scheda+Sigla Partito in bianco=totale elettori iscritti al seggio)

FPREF (preferenze)
Codice Seggio es: Gruppo/Regione/Provincia/Comune/Quartiere/Seggio**…** (immesso dal Seggio)
Codice del candidato (possibile che sia in + schede? e/o per + partiti?)
Partito di riferimento
Voti Digitali e Manuali

Il file FVOTI per 4-5000 elettori sarà di dimensioni assai modeste, attorno a 0,5 MB (almeno con gli standard di un tempo) e un solo server dovrebbe bastare per l'i.voting, ma con l'e.voting (voto digitale al seggio) non sarà possibile servire 5000 utenti con una sola macchina (10 ore = 36000 secondi : 5000 = 7 secondi per voto) quindi converrà che in ogni seggio *fisico* coesisteranno più seggi digitali con altrettanti PC (così come oggi esistono varie *cabine*).

Cosa succederà **nei giorni che precedono le elezioni**? (tanto nell'e.voting quanto nell'i.voting)

La procedura di aggancio al calcolatore centrale prevederà l'uso del Token (o di altro strumento) contenente l'**IP** del proprio seggio per richiamare il tabellone e le regole specifiche del seggio a cui si è iscritti. Le scelte verranno automaticamente trascritte in forma codificata **nella memoria del Token** (o altro)

Supponiamo che si voglia votare PXX alla Camera con preferenze per Mario e Paolo e PZZ alla Regione preferendo Toni: il software di scelta consentirà **di *cliccare* le proprie scelte direttamente a video** (evitando però scelte illogiche). Se poi, finite le elezioni, l'elettore intendesse verificare la presenza corretta del proprio voto nell'urna, **potrà** aggiungere anche una **sigla d'identificazione privata qualsiasi,** ad es. **MIASIGLA** (si userà in seguito questa parola *MIASIGLA* come *nome* dell'opzione)**.** Converrà che l'elettore non scelga sigle troppo banali (come pippo, pluto e topolino) però, se anche più elettori scegliessero la stessa sigla, resterà sempre possibile verificare se le proprie scelte

sono presenti in mezzo a quelle con ugual *MIASIGLA* (nel proprio seggio). Certo questa sigla, oltre a facilitare il voto di scambio, potrebbe anche essere usata per scrivere insolenze e porcherie che diventeranno pubbliche (e perché no? la gente ha diritto di dire quel che pensa, anche stupidaggini! Sarebbe *democratico* filtrarle? basterà proibirle ai minori ☺). Terminata la scelta il software presenterà il risultato delle scelte in questo modo:

MIASIGLA camera **PXX Mario** e **Paolo** regione **PZZ Toni**

e pure in forma codificata **MIASIGLA<1,PXX,1,3<2,PZZ,9** (regole di sintassi evidenti)

e il votante ricomincerà da capo se avesse cambiato idea. La riga **codificata** verrà mostrata anche quando si voterà non essendo impossibile che il votante abbia usato un programma fasullo che registri nella chiavetta (o in un dispositivo più funzionale) scelte diverse da quelle mostrate a video. Opportuno quindi controllare guardando nella chiavetta.

Evidente quindi che questa fase può essere eseguita in modo manuale (in caso di problemi o quando le scelte sono banali) utilizzando i codici mostrati fra parentesi nel tabellone (ovviamente pubblicizzato in strada e nei giornali). Il votante potrebbe scriverla come file di testo e copiarla nella sua chiavetta Non pare troppo complicato. Fuor di dubbio poi che nella cassetta della posta si troverebbero le stringhe suggerite dai candidati pronte per essere copiate (magari ci inviterebbero a pranzo dicendo di portare la chiavetta ☺). Sovente si vota genericamente per una organizzazione politica oppure si tratta di un ballottaggio o di un singolo referendum. Quindi non sono da escludere casi in cui è inutile appoggiarsi ad un "tabellone digitale", può essere più semplice immettere manualmente il voto in forma codificata, magari basterà SI o NO, 1 o 2, … Per facilitare questa ipotesi si potrebbero prevedere (dato il tabellone precedente) regole come le seguenti:

- l'indicazione di un solo partito (PZZ) sottintenderà un **voto generalizzato** (cioè PZZ = <1,PZZ<2,PZZ).
- in caso di scheda unica, accettabile anche PZZ,2 dove 2 indica una preferenza (anche più d'una)
- in caso di 3 **referendum** si potrebbe rispondere 1,SI 2,NO 3,NO e simili
- in un **ballottaggio** basterà scrivere 1 o 2 (se due sono i candidati)
- la stringa di controllo va però sempre separata dal resto con un <

MIASIGLA<PXX sarebbe l'esempio di un voto generico preceduto dalla sigla di controllo

In ogni caso:

- le schede non votate (previste dall'elezione) verranno considerate **voti bianchi** (<1 <2).
- invece i voti espressi indebitamente per limiti di età saranno cancellati (senza segnalare, visto che pare briga inutile).

Cosa succederà il **giorno delle elezioni?**

e.voting voto elettronico al Seggio in alternativa al **voto manuale con carta e matita**

In sintesi: **si mantiene il sistema attuale rendendo però rapido e sicuro il conteggio dei voti elettronici senza impedire ai diffidenti e agli anziani di votare nel modo consueto** (cosa concessa anche nel voto internettiano). Anche se il voto digitale è opzionale (si potrà decidere volta per volta entrando nel seggio) nell'ambito del singolo seggio la procedura di identificazione sarà digitale ed uguale per tutti; **potranno però coesistere seggi completamente tradizionali** (questo, come già anticipato, per consentire una conveniente gradualità di introduzione del sistema, quindi si potrebbe cominciare anche con un sol seggio digitale in tutta Italia).

PASSI

1) Durante le elezioni il **Seggio** viene presidiato dai **rappresentati di lista** e da un **tecnico informatico comunale**. All'apertura del seggio il computer (può essere un normale PC) viene ripulito di tutto, viene caricato il software necessario, viene caricato il file FTK (fornito dall'Anagrafe) e generato FVOTI in bianco, bianco (se possibile in doppia copia su dispositivi estraibili, anche solo due chiavette).

2) Arriva un elettore. I rappresentanti di lista inseriscono il Token (o altro), viene verificato se il seggio è giusto, se TK è presente in FTK (magari se ha la faccia giusta) e se non ha già votato. Se tutto OK il software chiede se si intende votare con carta e matita, se dice sì viene registrato M (eseguito voto) in FTK e l'elettore è invitato ad andare in cabina con carta e matita riprendendosi il Token. Il seggio annoterà il numero dei votanti manuali che non avessero ritirato o riconsegnato le schede di carta (per quadrare in numero di contrassegni M in FTK con le schede scrutinate). Il sistema stamperà su carta (e magari in un file corrispondente) anche i TK dell'elettore, questo per consentire di riportare manualmente (o automaticamente) questo M negli archivi di partenza qualora un *disastro* dovesse obbligare a ripetere le sole votazioni digitali. Al termine delle votazioni le schede manuali verranno aperte, controllate e totalizzate per essere poi aggiunte a mano ai file FSINT e FPREF (prevedibile quindi che i rappresentanti di lista solleciteranno l'elettore riluttante a servirsi del computer lì a sua disposizione aiutandolo in tutti i modi possibili e immaginabili ☺). Altrimenti:

3) viene messo un panno sul video, si inserisce la chiavetta e poi il personale del seggio si allontana; il votante toglie il panno e così vede la stringa del suo voto (ad es: **MIASIGLA<1,PXX,1,3<2,PZZ,9)** poi rimette il panno e dice se vuole proseguire (se rinuncia, potrà ricominciare da capo, magari a mano o preparando una nuova stringa di voto). Il personale del seggio pigierà un tasto corrispondente alla scelta.

4) Se prosegue, la stringa di voto viene registrata in FVOTI e si registra E in FTK . Se era presente MIASIGLA, questa viene crittografata dal server e trascritta assieme al voto nel Token (o in altro dispositivo). Critografata per evitare false lamentele a posteriori, vedi Passo 11.

oppure **i.voting via Internet,** ovunque ci si trova

Da verificare e completare col supporto di persone particolarmente esperte sulla sicurezza nella rete Internet.

Si tratta del voto elettronico in senso proprio**:** ovunque ci si trovi purché si abbia a disposizione un PC (o altro) connesso a Internet.

> NB la struttura destinata all'i.voting sarà utilizzabile per fare altre cose del genere: elezioni interne nelle organizzazioni politiche, nei sindacati, per le *primarie*, per raccogliere firme, per fare censimenti e magari affittato ai privati per fare indagini demoscopiche; tutto questo **diluirebbe i costi di gestione** ripartendoli sui più utilizzatori.

Si è già detto come potrebbe essere fatto il server di seggio per ridurre i rischi di intrusione, comunque converrà eliminare ogni dispositivo soggetto ad attacchi wireless, e ridurre all'essenziale il resto (quello che non c'è non si rompe e non può essere usato per fare brutti scherzi)**.** Si noti che per trovare l'eventuale grimaldello agli intrusi serve tempo e che si troveranno di fronte a un sistema **distribuito** e in funzione **solo per poche ore**. Tuttavia la questione non va presa sottogamba e dovrà essere attentamente considerata nello sviluppo software.

Come hardware basta una sola macchina per seggio e teoricamente di modestissima potenza e capacità perché i dati scambiati fra votante e server di seggio sono modestissimi; andrà però dotata di gruppo di continuità elettrica. Deve essere dimensionata per arrivare (nel tempo) a sopportare il traffico di 4-5000 voti nel tempo concesso per la fase 2. Chiamo **SS** il server del seggio collegato a Internet con **IP fisso** . Nei seggi vi saranno anche computer normali per consentire agli elettori di votare dal seggio come se fossero in remoto (ma, come detto, potranno votare anche con carta e matita).

PASSI

A) Come nel precedente Passo **1)** dell'e.voting; in più il programma di caricamento si collega ad Internet.

B) L'elettore o va a votare a mano in un seggio (Passo2 precedente) oppure inserisce il Token in un computer e il software del Token (o altro) si collega tramite l'IP a SS inviando il TK. Software attivo in SS cerca il TK in FTK, se non lo trova respinge il collegamento; se risulta *eseguito voto* avverte respingendo il collegamento. Se qualcuno (sicuro di non aver votato) ricevesse il messaggio di *voto già eseguito*, allora bisognerebbe pensare che gli avessero duplicato il Token. Al momento si ritiene che sia una possibilità da escludere. Dopo di che viene mostrato il voto al votante, ad es. **MIASIGLA<1,PXX,1,3<2,PZZ,9** e chiesto se si vuole proseguire. Se il votante risponde **NO** (per pentimento o evidenza di un imbroglio) la procedere viene interrotta. Altrimenti il software del Token (o altro) invia la stringa di voto a SS segnalando a video: *spedito, attendere conferma*.

C) Quando SS riceve la stringa, registra E (eseguito voto) in FTK e aggiunge la stringa di voto in **FVOTI** poi invia un byte che il software del Token decodificherà in *eseguito voto* nel video del votante. Se questa informazione di ritorno non pervenisse all'elettore (caduta della rete o del suo PC) e ritentasse l'operazione, verrebbe avvisato di *voto già eseguito*, in tal caso potrà solo verificare (a posteriori) se ciò è vero tramite l'eventuale **MIASIGLA** altrimenti non gli resta che lamentarsi col Comitato ☹ e/o con chi ha preparato la procedura e i programmi ☺ Se è presente MIASIGLA, questa viene **crittografata dal server** e trascritta assieme al voto nel Token (o altro dispositivo), la crittografia, durante il Passo 11, eviterà che vengano lanciate false accuse di alterazione dati allo scopo di invalidare le elezioni

- La stringa di voto viene pure scritta (anonima) dalla stampante del seggio per una evidenza della funzionalità del sistema e pure per consentire ai rappresentanti di lista di contare i voti a mano (a votazione chiusa) e di **essere così certi che dopo il ricevimento dei dati nessuno li ha modificati.**
- **Si ribadisce che TK e VOTO non coesistono nello stesso file garantendosi così l'anonimato nei supporti fisici, ma chi avesse accesso alla rete o alla memoria di SS durante le fasi B-C potrebbe forse abbinare TK e Voto (problema da valutare).**

E) Durante le votazioni, i rappresentanti di lista potranno eseguire operazioni di voto simulato usando un Token speciale capace di attivare speciali funzioni del software che mostrerà (sul video del server o su di una stampante dedicata) **la stringa immessa. Se i dati arrivano corretti è molto probabile che il sistema sia in ordine e che nessuno stia interferendo. Se intervenisse una manipolazione a posteriori, la totalizzazione manuale sulla base della lista cartacea dei voti ne darà evidenza.**

Cosa succederà **alla fine delle votazioni**? (tanto nell'e.voting quanto nell'i.voting)

5) Copie di FVOTI e della loro lista cartacea vengono consegnate ai rappresentanti di lista e altre copie saranno messe in una cassaforte apribile solo col consenso di tutti i rappresentanti di lista (da usare in caso di contestazioni).

6) Si fa lo scrutinio delle schede manuali (i totali saranno poi aggiunti a mano ai file FSINT e FPREF in **10**)

7) FVOTI viene *normalizzato* nel senso che potendo contenere informazioni scritte a mano con sintassi non standardizzata, la stringa viene trascritta (di fianco a quella originaria). Se si tratta di una normale elezione, supponendo ci siano due schede da votare, le regole del software del Seggio potrebbero essere :

- una singola stringa max 5 caratteri tipo PZZ o <PZZ viene tradotta in <1,PZZ<2,PZZ
- se non tutte le schede da votare sono state votate, verranno generati voti bianchi <1 o <2
- se tutta la stringa è bianca o non interpretabile, verranno generati voti bianchi per tutte le schede <1 <2
- partiti invalidi verranno ignorati, idem per le preferenze ignote o incompatibili col partito

- vengono cancellati (o non generati) i voti dati a schede non concesse per limiti di età.
Ad esempio, se si fosse digitato: **MIASIGLA<PZZ** la stringa diventa MIASIGLA<PZZ == <1,PZZ<2,PZZ
mentre: **MIASIGLA<1,PXX,1,3<2,PZZ,9** diventa MIASIGLA<1,PXX,1,3<2,PZZ,9 == <1,PXX,1,3<2,PZZ,9
(il campo di MIASIGLA andrà allargato al massimo concesso e la sigla allineata a sinistra del campo).
Naturalmente il tutto verrà reso pubblico (**11**)
Naturalmente i conteggi utilizzeranno solo la parte a destra di ==, mentre quella a sinistra (tutto ciò che è stato generato o scritto direttamente dall'elettore) sarà la chiave d'ordinamento-ricerca.

8) Un programma verificherà se il numero di voti in FVOTI corrisponde alle spunte fatte in FTK e quanti sono stati i voti manuali (per controllare con le schede consegnate).

9) Un programma legge FVOTI e ne deriva i file **FSINT e FPREF.** In FSINT viene aggiunto un record (privo di sigla di Partito) per ogni scheda indicante il n.ro totale degli aventi diritto desunto dalla lettura di. FTK Ad ogni record viene aggiunto il codice identificativo di seggio (che sarà di tipo *parlante* per fare le totalizzazioni territoriali richieste).

NB. Per eventuali altri dati statistici (età, sesso, … qui trascurati) eventualmente si faranno altre elaborazioni ripartendo dalla somma dei vari FVOTI che verranno raccolti dal Comitato interpartitico).

10) Con un apposito programma si aggiungono (a mano) i totali dei voti manuali (da **6**). Anche FSINT e FPREF vengono copiati e posti in cassaforte (in busta chiusa firmata da tutti). Una copia va al C**omitato Interpartitico** e magari anche al Ministero dell'Interno perché elaborino un primo risultato provvisorio (sono dati ancora soggetti a verifica e se anche qualche seggio avesse avuto problemi tali da dove rifare le votazioni, si possono comunque anticipare i dati salvo opposizione di almeno una delle organizzazioni politiche (che giudicasse troppo rilevanti l'entità dei voti in sospeso).

11) Il Seggio pubblica il file FVOTI in un suo sito in ordine alfabetico sulla stringa a sinistra di == in modo che si possa poter trovare rapidamente l'eventuale ***MIASIGLA*** e consentire ai votanti di verificare se il loro voto è stato recepito correttamente Bisogna però proteggere questo file dalle manipolazioni, al limite ricaricarlo frequentemente; una manipolazione non farebbe danni permanenti, ma creerebbe casino. Oppure il votante potrebbe chiedere al seggio l'invio del file FVOTI tramite una mail o andare al Seggio e copiarlo su propria chiavetta (potrebbe trattarsi anche solo di 1 MB!). Se il votante trovasse una divergenza, o non trovasse la sua MIASIGLA, il giorno stabilito può recarsi ad un seggio con Token dove è presente MIASIGLA crittografata, il seggio può decodificarla e verificare se il votante ha ragione. Se il votante non volesse perdere l'anonimato del suo voto potrebbe inserire il Token e un apposito programma potrebbe stampare il voto in busta chiusa, il votante apre la busta, controlla, richiude e la mette in una cassetta apposita. Al termine, le buste verranno aperte e si potranno constare le alterazioni (se si ritrovassero in pochi o soli, gli elettori potrebbero invece chiedere la distruzione delle buste per non perdere l'anonimato).

Qualora il file FVOTI venisse corretto (o addirittura rigenerato a seguito del rifacimento della votazione del Seggio) andranno rigenerati i file FSINT e FPREF (mantenendo i dati manuali immessi, vedere specifica procedura). L'evidenza di interferenze inaccettabili e il *peso* dei voti del seggio potrà indurre a rifare la votazione elettronica del seggio, oppure a rifarla totalmente con carta e matita se i problemi persistessero.

NB. Queste operazioni, utili per garantire la regolarità del voto, non sarebbero praticabili con un sol seggio centrale o con pochi di essi, peggio se in "cloud": ecco perché lo stato attuale di Internet sconsiglia sistemi troppo accentrati. Se gruppi pubblici o privati dicessero "stai tranquillo, controlliamo noi" io personalmente mi opporrei.

Cosa succederà **alla fine del tempo concesso per eventuali contestazioni**?

12) A questo punto i dati sono definitivi e risultati verranno mostrati. Chiunque potrà chiedere ad un seggio copia del file FVOTI e ricalcolarsi i dati esposti da FSINT e FPREF (ovviamente esclusi quelli manuali che restano, come oggi, garantiti dai rappresentanti di lista).

13) Il Comitato Interpartitico raccoglierà tutti i file FSINT e FPREF di tutti i seggi e ne ricaverà i Totali e Subtotali Definitivi (il Comitato li metterà tutti assieme in due file contenenti i record di tutti i seggi, chiamiamoli FSINTOT e FPREFTOT).

14) Chiunque potrà chiedere al Comitato copia dei file FSINTOT e FPREFTOT e ricalcolarsi i Totali e Subtotali Definitivi.

15) Se qualcuno avrà a ridire su qualcosa, lo farà sapere ai giornali e/o al Comitato il quale, essendo espressione di tutte le organizzazioni politiche, giudicherà insindacabilmente su quanto comunicato, potendo persino respingere le lamentele al mittente (i matti non mancano mai) e se qualcuno non fosse ugualmente contento, può sempre ricorrere ai forconi, nient'altro più esistendo.

NOTE

Voto di scambio

Oggi il problema dovrebbe essere meno sentito visto che non si danno le p**referenze** e questo semplifica assai la procedura di voto, perciò piuttosto che reintrodurle magari si potrebbe **dare ai cittadini la facoltà di licenziare gli indegni per via referendaria**, e di licenziarli alla svelta e senza attendere le lungaggini della magistratura (che ovviamente dovrà fare comunque il suo *lento* corso): se è vero che il potere spetta al popolo e che il politico esercita la sua funzione perché ha saputo conquistarsi il favore della gente, parrebbe logico dare alla stessa gente la facoltà di togliere ciò che è in suo potere (ovviamente per via referendaria). Oggi si sta andando proprio verso partiti personali, ballottaggi e presidenzialismo; inoltre affermare che **il potere spetta al popolo** e subito aggiungere **nell'ambito delle leggi che lo regolano** è un po' dare con una mano e con l'altra togliere.

Un altro sistema potrebbe essere quello di distribuire le poltrone minori come facevano gli Ateniesi: per sorteggio vedi https://blog.demarchia.info/ .

Permettetemi infine una riflessione delicata: se l'individuo è padrone del proprio voto, perché non può venderlo? Se la vedrà con la sua coscienza. **Quante cose facciamo tutti noi ben certi che, prescindendo dal nostro interesse, ci comporteremmo diversamente?** Quindi questo maggior rischio di voto di scambio mi pare solo una scusa per rifiutarsi di ragionare con la mente aperta sulla questione del "voto elettronico".

Altre considerazioni dello scettico citato all'inizio

A livello teorico una soluzione per assicurare l'invariabilità dei dati (in questo caso dei voti) esiste già, ma si scontra con diversi problemi di tipo pratico. Si tratta della famosa ***tecnologia blockchain*** *di cui tanti parlano ma che ben pochi capiscono. In parole povere si basa su una funzione di tipo crittografico che dato un input di lunghezza arbitraria produce un'impronta di lunghezza definita in output. In altre parole è una funzione di calcolo che genera una somma di controllo (checksum). Si dice che è crittografica perché è particolarmente robusta contro i tentativi di inversione, cioè dato un output è praticamente impossibile trovare l'input che l'ha generato, e perché dati input diversi è impossibile ottenere output uguali. Si inizializza la funzione crittografica in qualche modo e si ottiene la prima impronta. Dopodiché si concatena il voto di ciascun elettore con l'impronta ottenuta durante il ciclo precedente e si calcola quella nuova. Inizio = AAA -> AAA + voto1 = BBB -> BBB + voto2 = CCC -> CCC + voto3 ...*
Un sistema di questo tipo assicura che non si possano modificare voti lungo la "catena" e dato che si tratta di funzioni crittografiche si può essere certi che i voti siano effettivamente quelli espressi dato che voti diversi darebbero senza dubbio luogo a impronte diverse. A livello pratico però la soluzione è ancora lontana e si ritorna alle questioni di partenza. Come ci si assicura che votando il partito A venga davvero conteggiato un voto per quel partito anziché per il partito B? Un piccolo difetto (introdotto anche in buonafede) nel programma di voto già invaliderebbe tutta la teoria. Questo per non parlare di tutti i problemi connessi con l'inizializzazione sicura della catena, la trasmissione dei dati e via dicendo. Tutte queste funzioni si basano sulla robustezza degli algoritmi dimostrata a livello teorico, dando cioè per scontato che il "nemico" conosca come funzionano e che la sicurezza sia data solo dalla bontà dell'algoritmo stesso ed eventualmente dalla qualità della chiave. Con lo stesso approccio credo che si possa superare un buon numero di ostacoli, ma non ancora tutti e soprattutto non in modo immediatamente comprensibile e verificabile da chiunque, sia esso un elettore o un giudice.

> Concordo pienamente sulle perplessità: **la gente non si fiderà mai di una cosa gel genere, serve informatica semplice,** all'antica, che molti, con un po' di buona volontà, possano comprendere dalla A alla Z. E dove sarebbero i dati? Qua e là in "nuvole" sparse in tutto il mondo? No, meglio fare un passo alla volta, io comincerei coi metodi antichi (comunque assai più moderni della matita e soprattutto più comodi, efficaci e meno costosi) e poi si vedrà.

C'è anche da dire che le verifiche teoriche sugli algoritmi si basano sulle attuali conoscenze matematiche in merito, ma nulla ci garantisce che la CIA o qualche organizzazione analoga non abbiano scoperto un metodo innovativo che permetta di invertire delle funzioni ritenute non invertibili. Molti algoritmi di crittografia moderni si basano sulla fattorizzazione di numeri primi di migliaia di cifre: moltiplicare due numeri è facile, invece trovare i moltiplicandi che danno origine a un prodotto è un procedimento molto lento, cioè difficile. Se qualche matematico scopre un modo rapido per farlo molta crittografia corrente crolla come un castello di carte. Insomma, gli inglesi durante la seconda guerra mondiale avevano "risolto" la macchina Enigma tedesca e altre ben più complicate come la Lorenz però il fatto è stato rivelato solo 40 anni dopo. Nulla toglie che la CIA abbia già risolto alcuni dei problemi correnti, magari noi lo scopriremo fra 40 anni.

> Giustissimo, si pensi a cosa succederà coi calcolatori quantistici. Dicono però che si possano utilizzare cifrature non basate sui numeri primi e quindi non attaccabili per via quantistica. Altri escludono che Internet possa mai usare la quantistica. Comunque credo convenga cercare un rimedio "intrinseco" cioè un meccanismo che riduca di per sé i rischi ad un minimo tollerabile (la certezza assoluta nelle cose umane non esiste).

Gli americani intorno al 2006 riuscirono a mettere in piedi una complicatissima operazione di spionaggio informatico volta a danneggiare uno specifico tipo di centrifuga per la produzione di combustibile nucleare in uso in Iran. Un virus studiato apposta che seguendo un percorso incredibile aveva l'obiettivo di colpire un particolare pezzo di software in modo da far fare all'hardware delle centrifughe delle operazioni che le avrebbero danneggiate fisicamente, e tutto senza che i tecnici iraniani avessero alcun sospetto perché il software a loro faceva vedere valori diversi da quelli reali https://it.wikipedia.org/wiki/Stuxnet

Come già esposto nella proposta esistono i rimedi: **il broglio verrebbe scoperto e l'imbroglione resterebbe con un pugno di mosche.** Non ha senso faticare tanto se si è certi di essere scoperti, perciò si può stare relativamente tranquilli.

Alla fine per i governi è più facile influenzare il voto finanziando più o meno lecitamente campagne di disinformazione e contro-disinformazione.

Appunto, non avrebbero convenienza nel tentare di fare il mestiere degli hacker, ci rimetterebbero la faccia. Pur troppo **gli hacker esistono** e vorranno certamente far casino per il sol gusto di farlo: è da essi che io **vedo rischi per i quali servono competenze da aggiungere alle mie** (ne parlo nella procedura che si proposta). Si noti che la procedura limitata alla meccanizzazione del seggio (cioè senza l'uso di Internet) non avrebbe problemi e non capisco le problematiche USA (che si limitano a questo tipo di voto elettronico + le poste).

Resta il fatto che il voto elettronico è un ginepraio ancora senza soluzione, infatti è piuttosto difficile trovare informatici che lo consiglino a meno che non siano anche speculatori che su quel genere di software ci guadagnano un sacco di soldi perché fomentano le mire di politici che senza alcuna reale competenza tecnica vogliono introdurre il voto elettronico solo perché ha un'aria più moderna della vecchia carta e matita :)

Io sono un ex-informatico direi disinteressato e non propongo certo una cosa stile Casaleggio che fa un po' ridere se non piangere. Ho la presunzione d'intravedere una soluzione perché esco dagli schemi correnti. Una soluzione che si potrebbe testare spendendo poche migliaia di euro: perché non provare? O almeno, perché non valutare con attenzione e senza pregiudizi ciò che si propone?

Quanto all'identificazione del votante direi che la tecnologia aiuterà sempre più, si veda lo sviluppo del "riconoscimento facciale". Credo anche che presto sarà economicamente concepibile una specie di "telefonino" personale dedicato alla sola gestione elettorale semplificando enormemente tutta la questione. **Il vero problema da risolvere riguarda gli hacker: bisogna impedire che possano entrare come amministratori nei server di seggio e che distruggano o pasticcino i dati**

A sostegno del mio ottimismo ecco una corrispondenza con un informatico pratico di Linux

IO- Quello che ho trovato più interessante nei tuoi commenti è la possibilità di ritagliare un sistema operativo su misura, magari io mi illudo, ma forse questo potrebbe consentire di schivare qualcuna della trappole internettiane?

LUI- *In parte. Ti spiego meglio come funziona. Il fatto che Linux fosse open source ha fatto si' che la sua evoluzione fosse ramificata, come quella dei viventi. Per esempio, sul mio PC ho una Kubuntu, che e` una variante di Ubuntu, che deriva da Debian, che e` un Linux (sembra quasi di dire: mammifero, che appartiene ai vertebrati, che fanno parte dei cordati...). La maggior parte delle distribuzioni di Linux deriva da Debian o da RedHat. Sia Debian che RedHat hanno il concetto di pacchetto, anche se i pacchetti Debian sono diversi da quelli di RedHat. Tutto il sistema operativo e` fatto di pacchetti; gli applicativi utente installabili su una distribuzione di Linux sono pacchetti. C'e` un comando Linux per installare o disinstallare un pacchetto. Se un pacchetto ha bisogno di altri pacchetti per funzionare, il gestore dei pacchetti lo sa e installa anche quelli. Se vuoi farti un Linux ritagliato, installi un Linux minimale e poi aggiungi i pacchetti che ti servono, oppure parti da un Linux pieno e togli quello che non ti serve (puo` convenire l'una o l'altra strada a seconda dei casi; lo spartiacque in genere e` se ti serve il classico ambiente grafico a scrivania con finestre e mouse). Per quello che hai in mente credo che converrebbe partire da un Linux piccolo, eventualmente aggiungendoci a mano un piccolo X-window manager di base. Dato che, come dicevo, meno cose installi, meno bug introduci nel sistema, la sicurezza del sistema ne gode.*

Era appunto quello che speravo: nella mia procedura mouse e grafica servono solo nella visualizzazione del tabellone e per fare le scelte elettorali (ma queste cose le farei a parte con le tecnologie del momento, quindi non rientrano nella procedura), è nell'invio dei voti ai 'serverini' che ci possono restare problemi. Il mio vecchio ambiente IBM (RPG+SSP) era fatto di programmi complilati inseriti nelle ***procedure***: righe di comando che lanciavano programmi uno dopo l'altro, più eventuali programmi di sort e consentivano un po' di ***chiaccierare*** con l'utente, tipo: cosa vuoi fare? guarda che forse ti sbagli! ... e pure di fare qualche calcolino, il tutto riga per riga. A parte il collegamento con Internet lo spirito sarebbe quello.

Non prenderei invece in considerazione di ignorare Linux e farsi il proprio sistema operativo da zero. Ci ho pensato tante volte, mi sarebbe anche piaciuto farmi un sistemino operativo tutto mio,

quindi non lo giudichi impossibile

ma il problema e` costituito dai device driver. I produttori di hardware forniscono i driver per Windows, eventualmente qualcosa per Linux (che mi sembra vada forte in Cina; i cinesi non vogliono pagare per Windows). Tanti volontari nel tempo libero scrivono driver per Linux per l'hardware che vogliono usare e che il produttore non supporta. Non sempre la cosa funziona. Per esempio, ti assicuro per dolorosa esperienza personale che trovare una chiavetta USB WiFi moderna, che vada a 5 GHz, con driver per Linux e` un'impresa disperata. Linux e` quindi carente in driver (anche per colpa sua: praticamente ogni nuova versione di Linux e` incompatibile con i driver fatti per le versioni precedenti, che vanno quindi modificati, e questa e` una gigantesca fesseria; gli sviluppatori del kernel di Linux mancano completamente della mentalita` della compatibilita` all'indietro, anche se si illudono di averla),

mi rendo conto, ma quello che serve per il voto elettronico è pochissima roba e una volta fatta durerà assai a lungo e non richiederà aggiornamenti: se funzione oggi, funzionerà per lungo tempo: vero che dopo qualche anno un certa stampante non verrà più supportata, ma se fosse usata nei seggi (migliaia) resterà interessante per chi le vende o le mantiene.

ma qualcosa ha. Piu' di qualcosa. Ci si campa. Se ti fai un tuo sistema operativo, muori a fare i driver per ogni cosa. L'hardware va fuori produzione in continuazione. Se non continui a produrre nuovi driver per inseguire gli sviluppi hardware, ed e` un casino perche' spesso i produttori non rilasciano neanche una documentazione usabile, dopo qualche anno non e` piu' possibile reperire i componenti hardware supportati dal tuo sistema operativo e il progetto muore. Quindi sconsiglio l'approccio "tutto custom".

come già detto, questa procedura dovrebbe essere poco soggetta a modifiche: periferiche ne servono poche e assai modeste. Comunque un Linux ridotto (e quindi meno soggetto ad attacchi hacker) sembrerebbe già sufficiente. Purtroppo questo informatico non ha tempo per sviluppare una cosa del genere (inoltre risiede molto distante da me). Ho inutilmente sperato nei Grillini ai tempi del vaffanculo": ormai si sono convertiti alle convenzioni correnti e hanno relegato i loro sogni referendari ad una piattaforma "personale" e per niente trasparente.

Altre note

https://en.wikipedia.org/wiki/Operational_Control_Language **OCL** era il sistema operativo dei piccoli sistemi IBM, (SSP-RPG) comandi (interpretati al momento) che consentivano di interloquire con l'utente e di eseguire programmi in modo controllato (domande ed esecuzioni in base alla risposta, anche qualche calcolo) penso **potrebbe essere di ispirazione per la fase di invio del voto al server**, ovviamente mancava della comunicazione via Internet. SSP-RPG fu emulato sotto DOS dalla ditta LATTICE (quella del linguaggio c, **dispongo di questo emulatore**)

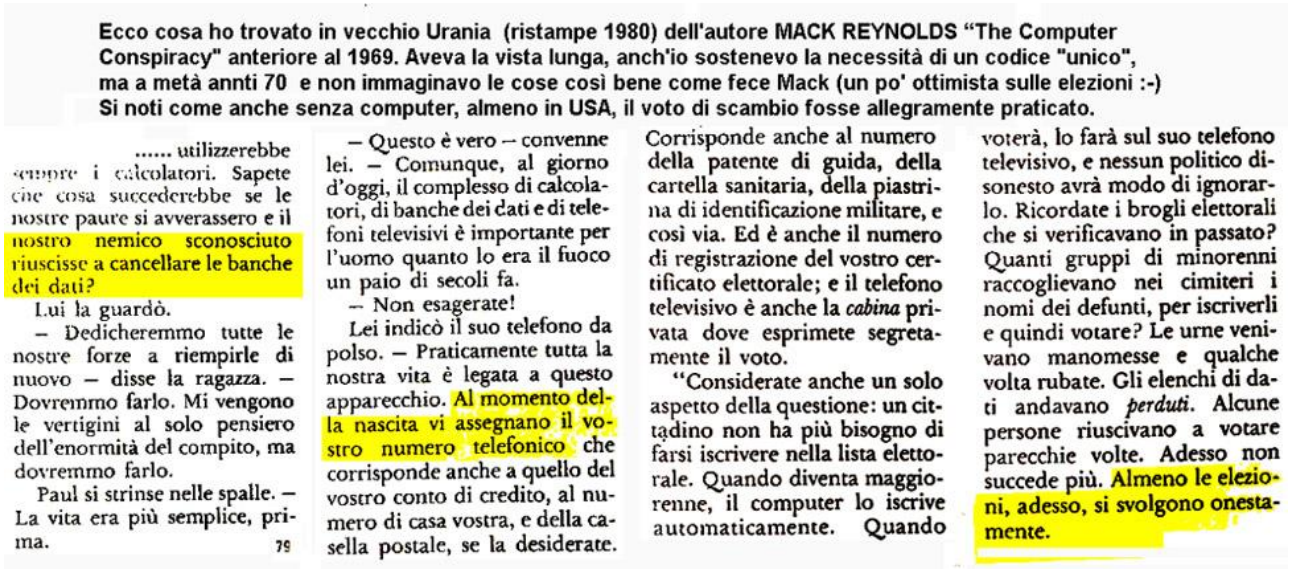
https://it.wikipedia.org/wiki/U3_(informatica) chiavette che lanciano programmi

Anche i guru informatici erano scettici, ma ora appare **Microsoft ElectionGuard** che fornirebbe sicurezza e controllabilità del voto tramite copie crittografate degli archivi (**ma se qualcuno li *cancellasse*?)**
https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-democratic-elections-through-secure-verifiable-voting/

https://www.repubblica.it/politica/2020/05/08/news/elezioni_una_piattaforma_gratuita_per_il_voto_online_sindaci_favorevoli_il_governo_la_adotti_-256049740/?ref=RHRS-BH-I0-C6-P6-S1.6-T1 il covid muove le acque: ma resto perplesso: se lo Spid risolve i problemi, perché hanno aspettato il covid? Lo Spid o qualcosa del genere era impensabile quando tutti i guru (a partire da Microsoft) dicevano che l'e.voting era impossibile?

http://amslaurea.unibo.it/1169/1/Varanelli_Francesco_Sistemi_per_il_pagamento_elettronico.pdf
http://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

Ecco cosa ho trovato in vecchio Urania (ristampe 1980) dell'autore MACK REYNOLDS "The Computer Conspiracy" anteriore al 1969. Aveva la vista lunga, anch'io sostenevo la necessità di un codice "unico", ma a metà annti 70 e non immaginavo le cose così bene come fece Mack (un po' ottimista sulle elezioni :-) Si noti come anche senza computer, almeno in USA, il voto di scambio fosse allegramente praticato.



..... utilizzerebbe sempre i calcolatori. Sapete che cosa succederebbe se le nostre paure si avverassero e il nostro nemico sconosciuto riuscisse a cancellare le banche dei dati?

Lui la guardò.

– Dedicheremmo tutte le nostre forze a riempirle di nuovo – disse la ragazza. – Dovremmo farlo. Mi vengono le vertigini al solo pensiero dell'enormità del compito, ma dovremmo farlo.

Paul si strinse nelle spalle. – La vita era più semplice, prima.

– Questo è vero – convenne lei. – Comunque, al giorno d'oggi, il complesso di calcolatori, di banche dei dati e di telefoni televisivi è importante per l'uomo quanto lo era il fuoco un paio di secoli fa.

– Non esagerate!

Lei indicò il suo telefono da polso. – Praticamente tutta la nostra vita è legata a questo apparecchio. Al momento della nascita vi assegnano il vostro numero telefonico che corrisponde anche a quello del vostro conto di credito, al numero di casa vostra, e della casella postale, se la desiderate. Corrisponde anche al numero della patente di guida, della cartella sanitaria, della piastrina di identificazione militare, e così via. Ed è anche il numero di registrazione del vostro certificato elettorale; e il telefono televisivo è anche la *cabina* privata dove esprimete segretamente il voto.

"Considerate anche un solo aspetto della questione: un cittadino non ha più bisogno di farsi iscrivere nella lista elettorale. Quando diventa maggiorenne, il computer lo iscrive automaticamente. Quando voterà, lo farà sul suo telefono televisivo, e nessun politico disonesto avrà modo di ignorarlo. Ricordate i brogli elettorali che si verificavano in passato? Quanti gruppi di minorenni raccoglievano nei cimiteri i nomi dei defunti, per iscriverli e quindi votare? Le urne venivano manomesse e qualche volta rubate. Gli elenchi di dati andavano *perduti*. Alcune persone riuscivano a votare parecchie volte. Adesso non succede più. Almeno le elezioni, adesso, si svolgono onestamente.

https://www.youtube.com/watch?v=GvPZe41S_as
dove Matteo Flora elenca i problemi del voto elettronico (a mio parere superabili come detto)