

Votazione elettronica e tecnologia nella democrazia moderna

E-Voting and technology in modern democracy

Nella maggior parte dei paesi, le elezioni si svolgono ancora nello stesso modo in cui sono state svolte per centinaia di anni, con carta e penna, in una cabina elettorale e organizzate centralmente dalle autorità locali.

Negli ultimi decenni, data la alta diffusione dei computer e delle migliori linee di comunicazione Internet, si è cominciato a prendere in seria considerazione il Voto Elettronico come al futuro della democrazia digitale o anche Democrazia Diretta Digitale (DDD).

E le consultazioni online sarebbero state all'ordine del giorno con la Democrazia Rappresentativa Digitale (DRD).

Cosa è successo da allora ad oggi ?

Cosa è cambiato ?

Purtroppo molti esperimenti sono falliti per gli alti costi e per la paura della sicurezza sui dati dei voti elettronici. Il problema principale, forse, è dovuto al numero di anomalie e all'incapacità di verificare che il voto contati siano effettiva espressione della volontà degli elettori e non dovuti a bug o manomissioni nel software o hardware utilizzato.

Molti paesi nel mondo hanno tentato il passaggio, e molti sono tornati alla carta. Alcuni hanno iniziato la sperimentazione.

Il Kenya ha rinunciato. Brasile, Venezuela, Paraguay, Panama, Costa Rica e Messico hanno implementato una qualche forma di voto elettronico. L'India lo ha esteso in tutto il paese.

Democracy Reporting International ritiene che il pericolo maggiore sia che questi governi vedono il voto elettronico come un proiettile d'argento per risolvere tutti i problemi elettorali. I governi quindi, deviano fondi pubblici in costosi esperimenti di voto elettronico, invece che su modi per eliminare problemi di scrutinio, intimidazione elettorale o violenze post elettorale. Il voto elettronico ha creato molte aspettative fino ad ora.

L'insidia è sempre la stessa, come per la carta: il broglio ed il controllo delle schede.

A questi ci si deve aggiungere il problema del controllo del software di voto, che non sia manomesso prima o durante il voto, oltre al problema della autenticazione di chi va a votare.

Se da una parte il voto elettronico permette di avere dalla sua il fatto che si estende il diritto di democrazia, facendo votare anche persone lontane o disabili, per esempio in paesi con vasta estensione territoriale e riduzione dei costi del personale di controllo ed in parte cartaceo, dall'altra molti pensano al rischio del controllo del voto, se chi vota sia veramente chi deve votare, o se vota secondo coscienza o sotto intimidazione diretta o indiretta, problematiche esistenti anche con il voto cartaceo, ricordiamocelo.

Le insidie del voto sono sempre le stesse, sia per un modo che per l'altro.

Quindi alla fine, cosa manca ? Sempre la stessa cosa, la **FIDUCIA**.

Il problema è che è un serpente che si morde la coda.

Democrazia, fiducia, diritti, sono tutte cose che dovrebbero andare di pari passo.

Purtroppo, nel tempo, molti hanno perso una delle tre, e spesso almeno 2.

Quando manca la fiducia, si perde almeno il diritto o la democrazia.

Quando si tratta di voto elettronico, devono essere affrontati molti problemi, alcuni tra questi sono: la sicurezza del software, la protezione contro il cracking e la garanzia che tutti i voti siano autorizzati e anonimi. Ora ci sono anche nuove tecniche crittografiche, come le **blockchain**, simili o uguali a quelle usate per la moneta elettronica o criptovalute, la più famosa è il Bitcoin.

Se i corridoi elettronici, quelli dove passano le informazioni, internet per intenderci, sono più sicuri con questo tipo di criptazione dei dati, cosa rende l'informazione sicura alla partenza e all'arrivo? Dovrebbe bastare la fiducia di chi vota e di chi controlla. Purtroppo non è così.

Quindi cosa si può fare ?

Si può fare un controllo sul software che ci permette di votare, in tempo reale, controllando che il codice non sia modificato e diverso da quello consentito e installato alla partenza.

Con software di controllo dell'integrità della memoria e dei programmi attivi necessari. Ma sono metodi che potrebbero essere costosi, e soprattutto occorre rendere sicuro il software fin dalla sua creazione altrimenti si rende vano tutto il processo.

Uno dei metodi possibili per rendere il software sicuro, è l'adozione di software **OpenSource**, dato che ha sorgenti pubblici, quindi controllabili da chiunque abbia la voglia di farlo, e per questo potenzialmente molto sicuro proprio perché non si può pensare che tutti i programmatori siano in malafede o comprabili o ricattabili tutti assieme, il numero elevato di questa tipologia di persone assicura un maggiore etica e controllo del sorgente. Nuovi software OpenSource per il voto elettronico stanno nascendo e con essi nuovi metodi di sicurezza.

Un esempio lo sta dando il West Virginia, che ha appena annunciato che amplierà il suo uso del voto elettronico nelle elezioni presidenziali del 2020. La distribuzione sarà ancora molto limitata e disponibile solo per gli elettori disabili, ma è comunque una mossa ambiziosa che sta attirando l'attenzione e le critiche.

Anche le soluzioni decentralizzate di e-voting sono particolarmente interessanti in quanto possono offrire soluzioni a problemi come verificabilità e sicurezza. Gli elettori possono verificare che il loro voto sia stato gestito in modo equo e corretto: non è necessario affidarsi a istituzioni o funzionari dedicati per valutare i voti.

Purtroppo, casi di insuccesso dovuti a cause non imputabili al software, ma errori umani di comprensione del suo utilizzo, capitano e non danno comunque fiducia al voto elettronico, anche se il problema è puramente umano senza malizia di intenti.

Un altro rischio è quello che per risparmiare dei soldi, abbassando i costi del voto con il voto elettronico, si aprono le porte per una possibile dittatura eterna.

La **FIDUCIA** è cruciale per l'accettazione del voto elettronico per le elezioni future.

I SOFTWARE

Tra i **software** per la decisioni di Democrazia Digitale, vanno citati:

- 1- **Liquid Feedback** o **LQFB**, introdotto ed usato principalmente dal Partito Pirata.
- 2- **Decide Madrid**, usato principalmente in Spagna.
- 3- **DEVOTEE**, un sistema di voto elettronico per le decisioni del rilascio e modifica del software (usato da **Debian**, un sistema Operativo Linux).

1- Le premesse per **LQFB**, software OpenSource, sono di avere una **Democrazia Liquida**, che permette di non centralizzare il potere su una persona o su un gruppo, ma su tutta la collettività dei partecipanti. Quest'ultima include contemporaneamente i concetti di democrazia rappresentativa e democrazia diretta. Ed in questo modo si evita di cadere nel tranello della deriva oligarchica dei partiti, in cui si segue un leader o un gruppo centrale di persone, che decidono, di fatto, le linee guida del partito scavalcando le idee delle persone.

Perché l'idea alla base è che la collettività pensa meglio per il bene della collettività stessa, di quanto lo possa fare un singolo individuo o un gruppo ristretto di persone.

LQFB ha anche la **DELEGA** di voto. La delega è dare fiducia completa al delegato. La delega di voto viene usata per: proposte di legge, linee guida del partito, aderire ad iniziative e simili, e per ambiti in cui il delegato è più esperto di noi (informatica, legge, cultura, architettura, etc...), ma non per le cariche interne, questo perché i voti devono essere disgiunti dalla singola persona che ha una o più deleghe, così che ogni singolo partecipante si prenda la sua responsabilità di voto.

Una testa un voto in questo caso.

In LQFB, il voto finale NON è segreto, così che si possa verificare che il proprio voto sia andato nel posto giusto, e poter verificare che tutto sia corretto.

In qualsiasi momento si può togliere la delega, sia perché per quella votazione vogliamo essere noi a di SI o NO, e poi ridare la delega, sia se si scopre che il delegato non ha votato secondo le linee di pensiero comune, e si toglie la delega per sempre, perché ha perso la nostra fiducia.

Tutto questo, ogni singola modalità di funzionamento e decisionale, può essere implementato via software all'interno della piattaforma digitale di LQFB.

La delega di voto, per le votazioni pubbliche di stato, non è, per ovvie ragioni di segretezza, da usare ed usabile. Il voto per votazioni di stato, deve essere e restare segreto, e non è quindi possibile dare deleghe. Sarebbe come se per andare in cabina elettorale, invece che andarci Mario Rossi e votare A, ci va Fabio Verdi che voterà anche per noi, e che dovrebbe votare A (ma potrebbe anche votare B). Noi, avendo dato delega di voto, non sapremo mai come voterà effettivamente la persona a cui affidiamo la delega, anche se ha la nostra fiducia e pensiamo che voti come noi o con il suo pensiero di cui ci fidiamo; votare SI o NO per approvare una legge, fare eleggere Tizio o Sempronio, è diverso che dare il parere per una proposta di legge od una opinione su una tematica.

Comunque, LQFB è più usato all'interno del partito e non per votazioni di stato.

Può essere usato per le votazioni e situazioni che non hanno problemi di segretezza del voto.

2- Anche **Decide Madrid** è un ottimo software OpenSource per le votazioni elettroniche, già usato in Spagna, con molto successo, ed adottato da varie province spagnole.

Decide Madrid è un software completo per il voto elettronico e per le decisioni democratiche. Offre strumenti informatici come: le Assemblee Cittadine, la Giuria Cittadina, Pianificazione delle Azioni (metodo strategico per focalizzare e decidere i passi da intraprendere per raggiungere certi obiettivi), le Town Meeting (per discutere problemi locali, regionali e nazionali).

Decide Madrid cerca di mettere le persone al centro del processo decisionale, per costruire una democrazia più forte che funzioni per tutti, che dia alle persone il potere reale di portare un cambiamento nella loro vita, comunità e oltre.

A livello decisionale è, in linea di massima, come LQFB e permette di raggiungere una decisione collettiva, che va bene a tutti; a livello di voto elettronico, ha già tutte le caratteristiche ottime per poter essere usato in larga scala.

Forse, e dico forse, gli mancano solo le nuove tecnologie di blockchain, che comunque, possono essere implementate con una nuova versione del software.

3- **Debian** con **DEVOTEE (DEbian VOTe EnginE)** usa il metodo Schulze.

Il **metodo Schulze** è un sistema di valutazione dei voti sviluppato nel 1997 da [Markus Schulze](#) che seleziona un singolo vincitore utilizzando i voti di preferenza. Il metodo può anche essere utilizzato per creare una lista di vincitori. È considerato una variante del [metodo di Condorcet](#).

Il metodo Schulze è utilizzato da numerose organizzazioni tra queste: [Software in the Public Interest](#), [Debian](#), [Gentoo](#), [Wikimedia](#), [KDE](#), [Free Software Foundation Europe](#), [Partito Pirata Svedese](#), [Partito Pirata Tedesco](#), [Partito Pirata Italiano](#), [Podemos](#).

In pratica Debian con Devotee, ha un sistema di tracciamento dei voti che fornisce lo stato delle risoluzioni generali in corso e i risultati dei voti precedenti. Debian usa il metodo Condorcet per le elezioni del leader del progetto.

Semplicisticamente, il metodo Condorcet può essere affermato in questo modo:

- Considera tutte le possibili gare a doppio senso tra candidati. Il vincitore del Condorcet, se ce n'è uno, è l'unico candidato che può battere l'altro candidato in una gara a doppio senso con quel candidato.

Il metodo di voto per il metodo Schulze è lo stesso di altri metodi elettorali [preferenziali](#): ogni votante deve fornire una [lista ordinata di preferenze](#) per i candidati.

Con l'aumentare delle opzioni votabili (tre, quattro,...) la lista può allungarsi, comprendendo opzioni giudicate sullo stesso piano; ad esempio ordinando la lista così:

$A > B > C$ e $D > E$ e $F > G$

Un esempio molto semplicistico del metodo, a termine votazioni le liste di preferenza appaiono così (per ogni votante):

1. $A > B > C > D$;
2. $A > B > D > C$;
3. $D > C > B > A$;
4. $B > C > D > A$;
5. $C > B > D > A$.

Il risultato del voto sarà pertanto: $B=10, C=8, D=6, A=6 \rightarrow B > C > A$ e D

Quindi vince B.

Inoltre, in caso di voto segreto, viene fornito un codice univoco, solo al votante, per verificare che il voto espresso dal votante, sia come voleva che fosse subito dopo aver votato e dopo le votazioni finali.

Si rimanda alla wiki o sito Debian per eventuali approfondimenti sia del metodo [Shulze](#) che di [DEVOTEE](#).

TECNOLOGIE di CRIPTAZIONE

Tra le tecniche di criptazione, l'adozione di tecnologie **BLOCKCHAIN** a livello globale è ormai partita ed inevitabile.

Tra le nuove tecnologie emergenti, ricordiamo i software **TEZOS** e **ALSTRIA**, ma non sono gli unici che si stanno affacciando sullo scenario del voto elettronico OpenSource.

Cosa permette a **TEZOS** di essere avanti rispetto ad altri ?

Tezos usa il protocollo **E-CLESSIA**, promosso dalla organizzazione no-profit Electis, che esplora e promuove tecnologie per il voto elettronico o democrazia elettronica e rafforzamento della democrazia, mantenendola al contempo sicura, trasparente e rendendola accessibile a tutti.

Electis sta sviluppando e testando il voto con blockchain con le università, poiché la fiducia nel sistema è fondamentale in qualsiasi elezione, ed è importante coinvolgere i cittadini in questi

progetti e provare nuove tecnologie in contesti a basso interesse e aperti al mondo accademico e al pubblico.

Tezos con il Self-Amendment, On-Chain Governance e la Decentralized Innovation, evita lo sdoppiamento del progetto in due o più rami distinti, ma simili, così da non diminuire le forze ad esso dedicate, lavorando tutti ad un unico progetto si ha più forza lavoro sia fisica che mentale; le parti interessate possono partecipare e proporre emendamenti, modifiche al protocollo, incoraggiando, in questo modo, la partecipazione e facilitando lo sviluppo e l'adozione di Tezos, raggiungendo un accordo complessivamente accettato da tutti i partecipanti.

Tezos permette anche la **DELEGA** di voto, e per incentivare la onestà e disincentivare la disonestà, viene richiesto il deposito cauzionale (evitando che venga diluito dall'inflazione).

Se un partecipante si comporta in modo disonesto, può perdere il proprio deposito.

Gli utenti che non desiderano partecipare direttamente alle votazioni, possono delegare altri utenti a farlo per conto loro. Delega che può essere inibita o tolta per votazioni importanti come quelle elettorali cittadine o del paese.

Tezos è usabile sia a livello cittadino che governativo ed anche a livello bancario, per il protocollo di sicurezza implementato.

Parte della sicurezza di Tezos è dovuta alla decentralizzazione dei server, in questo modo, non si ha una connessione peer-to-peer, ma in stile bittorrent per intendersi, appunto decentralizzato, con una distribuzione senza confini e senza server centrali controllabili, inoltre con il protocollo di sicurezza basato su blockchain, è estremamente difficile, se non impossibile, contraffare lo scambio di dati.

Che cosa è **ALASTRIA** ?

E' un consorzio che promuove l'economia digitale attraverso lo sviluppo di tecnologie di registrazione decentralizzato basate su blockchain, che vuole creare un sistema usabile sia dai governi che dalle banche.

Sulla scia di Decide Madrid e dopo che è uscita la notizia che Mosca sta lanciando la sua crypto valuta (CryptoRuble), in Spagna nasce (2017) questo consorzio atto a sviluppare un libro mastro cittadino sulle blockchain. Il consorzio è formato da privati (aziende di energia, telecomunicazioni e finanza), e enti pubblici (governo ed università).

Alastria dà spazio anche alla IDENTITÀ' Digitale (ID Alastria) creando quindi uno standard, seguendo le linee guida della Unione Europea sui dati personali dei cittadini (che ne hanno il pieno controllo) e la trasparenza.

CONSIDERAZIONI FINALI

Data l'emergenza globale in cui viviamo in questi primi mesi del 2020, e di cui ancora non si sa la fine, è ovvio che occorre pensare, ancora più di prima e forse con più urgenza, ad un sistema globale di criptazione dei dati sicuro, sia per le transazioni elettroniche che per il VOTO ELETTRONICO.

Perché anche se si può mettere in pausa per un po di tempo l'economia, con le dovute precauzioni di salvaguardia se si vuole che il sistema economico si possa riprendere (vedi Grecia qualche anno fa), la democrazia e lo stato di diritto, il funzionamento dei governi non può e non deve fermarsi.

Per quanto ci sia una eccezione, il Belgio, che è cresciuto economicamente quando i governi sono caduti ed il sistema Belgio è stato retto da un governo temporaneo non eletto per 540 gg.

Un esempio lo abbiamo qui in Italia, proprio ora. Un referendum sul “taglio dei parlamentari” che doveva svolgersi il 29 marzo 2020, è stato rinviato a data da destinarsi, perché in Italia esiste solo il voto fisico, con la carta, recandosi alle urne, e quello via posta è usato solo per i residenti all'estero. Questa metodologia di voto, oltre ad avere costi elevati, ed a fermare le scuole e l'istruzione, perché le scuole sono il luogo più usato per effettuare le votazioni in Italia, essendo gli edifici più diffusi e disponibili per una tale movimentazione cittadina, blocca anche il diritto di voto. Anche se un tempo, in Italia, si usavano Comuni, Caserme e posti di polizia. Se invece avessimo la possibilità di fare in modo sicuro ed accettato da tutti il voto elettronico, potremmo svolgere molte attività di voto e democrazia, senza dover aspettare di poter uscire di casa e chiudere le scuole, e con costi inferiori; comunque, anche a costi paritari o superiori, la democrazia andrebbe avanti e non verrebbe bloccata come accade ora, in cui lo stato di diritto viene fortemente limitato. Se almeno potessimo fare delle votazioni elettroniche, parte del diritto che noi possiamo esercitare verrebbe portato avanti.

Uno dei problemi del voto elettronico, ma anche cartaceo ovviamente, è la possibile MANIPOLAZIONE della opinione dei cittadini da parte delle TV e dei giornali, dei media in generale, prima di una votazione, che può influenzare il voto per un referendum o altro, spostandolo in una direzione o l'altra.

Ad esempio, si pensi all'esito diverso che può dare un referendum sulla pena di morte se poco prima delle votazioni si fanno vedere gli atti di un pericoloso omicida o si da notizia della scoperta del vero responsabile di un omicidio, al posto del quale un'altra persona era stata mandata pochi giorni prima sulla sedia elettrica.

Per questo, occorre una chiara e precisa indicazione di come e quando parlare dell'argomento del voto, prima della tornata elettorale, proprio come per il voto cartaceo.

E magari unendo il voto elettronico a votazioni classiche cartacee (referendum o elezioni che siano), avendo fatto informazione per impedire un abuso di informazioni a scapito della comprensione del quesito e ad una manipolata informazione .

Quindi occorre informazione per gli elettori/votanti , in modo che le persone si formino una opinione con informazione neutra, con pro e contro alla domanda posta in referendum, un Libretto/Opuscolo Informativo in stile Svizzero o Oregon per esempio.

Prevedendo per esempio, i referendum in particolari giorni dell'anno o in coincidenza con elezioni politiche, in questo modo il voto referendario è preceduto da una fase abbastanza lunga di informazione e riflessione che permette di epurare dati emozionali più forti dal voto ed impedire un abuso di informazioni a scapito della comprensione del quesito e ad una manipolata informazione.

Citazione dal libro: Iperdemocrazia: Come cambia la sovranità democratica con il web – Rodotà - Laterza – 2013 - cap.4 – Referendum Elettronici.

Il Sondaggio o Sondocrazia:

“Ora, vincoli tecnici a parte (come quelli che condizionano la formulazione e l'esplicazione delle alternative al numero di caratteri che possono apparire sullo schermo), questa procedura pone problemi sia nella sua fase preliminare, che riguarda la scelta del tema da sottoporre a referendum e, soprattutto, nel momento della scelta delle alternative da proporre ai cittadini. Se, ad esempio, si affronta il tema dei tossicodipendenti, si può chiedere ai cittadini di scegliere tra una politica che preveda il loro arresto, una che preferisca il loro ricovero coatto in un ospedale ed una che punti ad allontanarli il più possibile dalla città considerata. La soluzione scelta dai cittadini potrà essere presentata come quella corrispondente all'opinione della maggioranza, e dunque come la più democratica. Ma ai cittadini non è stato chiesto, ad esempio, se preferivano una politica di prevenzione, di cura volontaria, di graduale reinserimento dei tossicodipendenti nella comunità. Uno schema così

semplificato – e ancor più quello referendario secco, che ha come unico sbocco la scelta tra un SI e un NO – può dunque tradursi in una pericolosa riduzione dell'area delle scelte dei cittadini, cancellando in modo autoritario (o almeno arbitrario) alternative che pure sono realisticamente proponibili. Il rischio, allora, diventa quello di un'eclissi della democrazia pluralista, visto che può essere preclusa la stessa possibilità di valutazione collettiva di soluzioni che una parte dei cittadini ritiene preferibili. Può, anzi, essere negato uno dei caratteri stessi della democrazia, intesa come un regime che garantisce la non esclusione di alcun tema dalla possibilità di discussione e decisione.

Le nuove possibilità tecnologiche assegnano al referendum un ruolo prima impensabile, per la rapidità e la frequenza con cui diventa possibile ricorrere ad esso. Scompare ogni possibile mediatore sociale. La casa/terminale elettronico può essere trasformata in una cabina elettorale permanente. Privata del confronto e della comunicazione reciproca, circoscritta al gioco della domanda e della risposta, la nuova democrazia di massa assumerà i caratteri di una living room democracy, di una soffocante «democrazia del tinello»? (fine cit.)

Queste parole ci devono fare riflettere attentamente sul voto elettronico.

Occorre quindi fare molta attenzione al definire correttamente l'uso del voto elettronico e fare sì che non diventi mera illusoria garanzia di democraticità, dovuto al flusso di comunicazioni dei media e non alla necessità specifiche dei cittadini, chiamati a dare risposte a questioni politicamente rilevanti.

Occorre anche fare molta attenzione che l'innovazione tecnologica non tenda prima di tutto a risolversi in un rafforzamento delle posizioni di potere già esistenti, lobbies e altro.

Un altro problema di cui tenere conto, è il tema della 'alfabetizzazione' dei cittadini, dunque la necessità di diffondere la conoscenza delle nuove tecnologie e della loro modalità d'uso, se non si vuole avviare un processo di esclusione e dunque di riduzione della democrazia. Occorre anche individuare risorse che, oltre che alfabetizzare, aumentino il livello di istruzione e di reddito, in modo che non divengano anch'esse veicolo di esclusione e non influenzino la partecipazione politica. Ampliando la possibilità di intervento dei cittadini, si possono avviare processi di apprendimento sociale, stimolando la partecipazione di individui e gruppi, non più in posizione marginale o subordinata come nei procedimenti di decisione a piramide. Viene così favorito il confronto tra proposte alternative, di cui è anche incentivata la formulazione.

Cit: "La conoscenza crea le condizioni perché altri soggetti entrino da protagonisti nell'arena politica."

Ecco perché il Voto Elettronico è da prendere non solo in considerazione, ma da sviluppare in maniera ancora più aggressiva, per dare modo ai cittadini di esprimere il proprio voto. Ricordandoci che alle porte c'è sempre la possibilità di una deriva dittatoriale se non si fa un uso corretto dello strumento, come per tutti gli strumenti decisionali.

Dobbiamo anche considerare che la Democrazia ha un costo, e ne va tenuto conto, e non si può rinunciare alla democrazia per ridurre il costo dei sistemi elettorali, quali essi siano, cartacei o elettronici.

Occorre quindi tenere ben a mente i vantaggi e gli oneri che la democrazia porta con se.

Ricordiamo che questo non è un elenco esaustivo dei vari metodi e software usabili, ma deve essere un esempio base, uno spunto per ragionare sulla metodologia e sulla fattibilità del voto elettronico.