Votazioni americane e tecnologia blockchain: un matrimonio impossibile?

di Patrizio Rubechini

pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale - 19 gennaio 2021

Mentre Trump ancora combatte con le corti statali nel tentativo di ribaltare gli esiti delle elezioni che hanno visto prevalere nettamente lo sfidante Biden, negli USA torna prepotentemente di attualità il tema dell'innovazione del sistema di voto: infatti, nel paese che affianca alla tradizionale votazione "in presenza" il discusso voto "postale", molte sono le sollecitazioni alla politica affinché venga implementato un modello digitale sicuro per la gestione dei voti e la rendicontazione pressoché immediata dei risultati. Ma non è tutto oro ciò che riluce, e diverse sono le questioni problematiche.

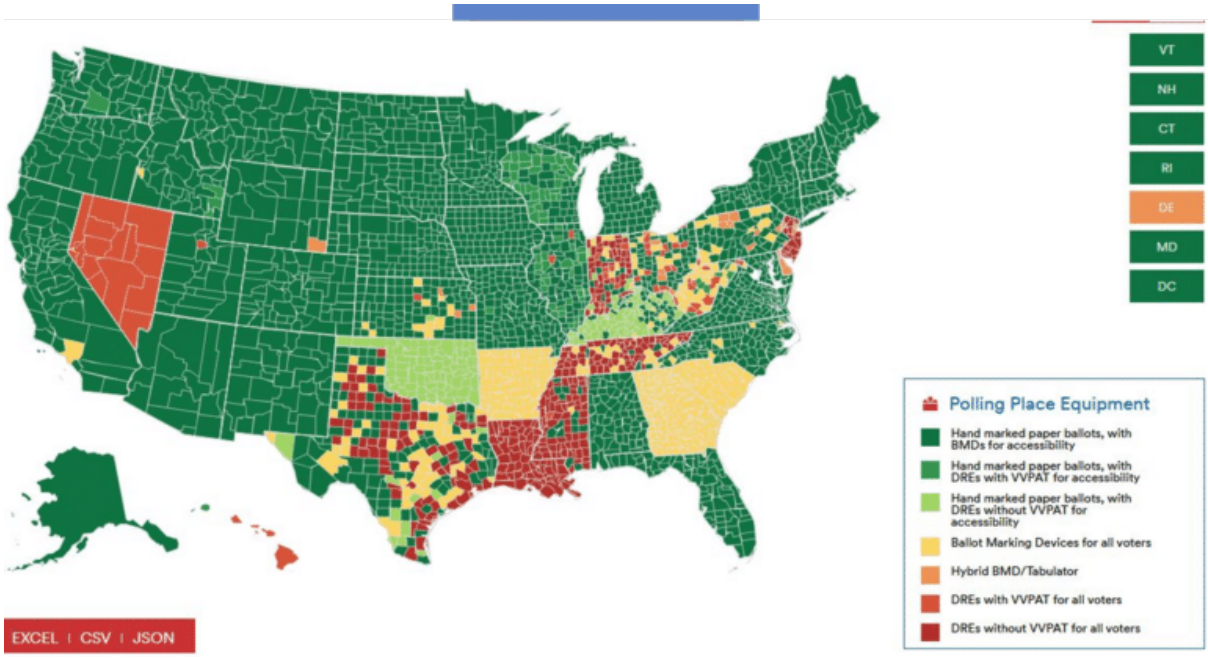
Gli Stati Uniti sono, tra i paesi del mondo occidentale, uno dei primi ad aver adottato sistemi di votazione a base elettronica (c.d. *e-voting*) o, comunque, semi automatizzata: in principio furono le schede perforate, seguite dai lettori ottici e, in ultimo, dai sistemi di registrazione elettronica diretta che attualmente utilizzano addirittura postazioni di voto "*touch*".

Solo l'Estonia può considerarsi realmente più avanzata nel settore, dal momento che lì si vota *online* (c.d. *i-voting*) in pianta stabile già dal 2014. Anche le recenti elezioni parlamentari del 2019, ad esempio, si sono svolte *online* e hanno costituito l'occasione per una interessante analisi delle procedure elettorali adottate, svolta dall'OSCE e contenuta nel Rapporto stilato dall'Office for Democratic Institutions and Human Rights).

L'attuale sistema di votazione americano, del resto, continua ad accusare due rilevanti punti deboli.

Da un lato, la coesistenza – sia all'interno del singolo Stato federato che tra i vari Stati – di modalità di votazione profondamente differenti, di certo non favorisce l'uniformità e la standardizzazione del sistema. Accanto al tradizionale voto cartaceo (c.d. "*hand marked paper ballots*"), adottato in tutti gli USA tranne South Carolina, Georgia, Arkansas e Delaware, ritroviamo infatti sia i c.d. "*ballot marking devices*" (BMD) ovvero sistemi elettronici ad elevata accessibilità in grado di restituire comunque una traccia cartacea del voto (come ad esempio in South Carolina, Georgia, Arkansas, Delaware, Texas, Ohio, Pennsylvania, Indiana, California), che i c.d. "*direct recording electronic systems*" (DREs) ovvero apparati che consentono l'espressione e la registrazione del voto interamente su base elettronica (come ad esempio in Louisiana, dove questo sistema è utilizzato in maniera esclusiva, o in Nevada, Tennessee, Mississipi e New Jersey, dove i DREs si affiancano agli altri sistemi).

Dall'altro lato, invece, si assiste alla generale necessità della presenza fisica del soggetto votante presso le urne, condizione questa che, di fatto, riduce di molto la portata innovativa delle metodologie elettroniche appena descritte.



Il tutto senza mai dimenticare la problematica eccezione rappresentata dal voto postale (largamente diffuso in California, Colorado, Hawaii, Nevada, New Jersey, Oregon, Utah, Vermont e Washington), che di fatto è un voto "*hand marked*" ma, nel contempo, è anche una primitiva forma di voto a distanza.

In altri termini, l'attuale sistema di votazione adottato dagli USA si risolve in una complessa congerie di differenti modelli operativi, la cui gestione concreta è sostanzialmente lasciata ai singoli Stati federati, ciò che ha contribuito fortemente ad alimentare le polemiche sollevate da alcune parti politiche sulla affidabilità dei recenti risultati elettorali delle presidenziali 2020.

Per queste ragioni, da diverso tempo il voto digitale via Internet (c.d. *i-voting*) applicato alla tecnologia *blockchain* viene visto come la soluzione ideale e definitiva al problema: l'adozione della tecnologia *blockchain*, infatti, porterebbe con sé la sicurezza e l'impenetrabilità dei dati, che è la cifra tipica dei sistemi "a registro distribuito", mentre la possibilità di un voto a distanza diffuso – grazie anche alla vasta fruizione della tecnologia Internet sul territorio americano (tra l'80 e il 100% della popolazione servita) – risolverebbe d'un tratto le critiche legate alla scarsa trasparenza e alla presunta modificabilità a posteriori di un voto per posta che, per evidenti limiti strutturali e fisici, soffre il ritardo nella fase di conteggio che deriva dai tempi necessari per il trasporto delle schede.

Un futuro sistema diffuso di votazione basato su *blockchain*, pertanto, potrebbe avere come caratteristiche "di base" quella di svolgersi a distanza per il tramite della

rete Internet (questo renderebbe possibile il "voto da casa", ma anche dal posto di lavoro o dal proprio smartphone senza però dover eliminare del tutto il seggio elettorale "fisico", ultimo presidio delle fasce di popolazione non digitalmente alfabetizzata) e di utilizzare metodi digitali di acquisizione e archiviazione delle espressioni di voto (tramite, ad esempio, le descritte tecnologie BMD o DREs, o più semplicemente attraverso la conversione del voto cartaceo in dato informatico).

Esso, inoltre, andrebbe a costituire una specifica variante di voto elettronico, pur potendo comunque rimanere limitato a fungere da sistema di conservazione digitale dell'espressione di voto (financo di quella semplicemente cartacea e successivamente convertita in un dato digitale).

Questo perchè la *blockchain*, laddove applicata ai sistemi di voto, non inciderà mai nella fase iniziale della sua espressione (che potrà rimanere "in presenza" presso le urne o, con maggiore probabilità, svolgersi a distanza attraverso la rete Internet), ma opererà principalmente nelle fasi successive di elaborazione, rendicontazione, trasmissione e conservazione dei dati, rendendole estremamente più sicure dal punto di vista di possibili intrusioni informatiche finalizzate alla manipolazione fraudolenta.

Agli entusiasmi dei "tecnologisti" si è però contrapposto un nutrito gruppo di scienziati e ricercatori dell'autorevole AAAS – American Association for the Advancement of Science che, con una lettera aperta ai governatori e alla Segreteria di Stato, ha messo nero su bianco una serie di perplessità e di potenziali punti critici che deriverebbero dall'eventuale implementazione del voto via Internet:

a) i sistemi di voto via Internet sono attualmente non sicuri e non esiste alcuna evidenza tecnica del fatto che possano diventarlo a breve, anzi è vero il contrario;

b) la tecnologia *blockchain* non può mitigare o compensare i pericoli derivanti dal voto via Internet;

c) nemmeno i sistemi mobili di voto via app garantiscono un sufficiente livello di sicurezza dell'espressione di voto.

Secondo l'AAAS, Internet – e di conseguenza qualunque tecnologia che vi si appoggi – presenta rilevanti vulnerabilità legate alla elevata diffusibilità di malware, all'esposizione ad attacchi massivi (i c.d. attacchi DoS – *denial of service*), all'affidabilità nella fase di autenticazione dell'elettore, alla sicurezza e anonimizzazione dei voti registrati e alla successiva fase di *audit* e di materiale riconteggio dei voti nel caso di contestazioni elettorali, quest'ultima resa assai critica dalla mancanza – nei sistemi di *e-voting*/*i-voting* interamente digitalizzati – di un supporto cartaceo verificabile.

Già nel 2018, tra l'altro, la National Academies of Science, Engineering, and Medicine (NASEM) aveva messo in guardia le istituzione americane con un *consensus study report* dal contenuto riassumibile in un breve ma significativo passaggio: "*At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet*".

D'altra parte, per quanto la tecnologia a registri distribuiti risulti in grado di assicurare elevati standard nella fase di memorizzazione e conservazione dei dati di voto, criticità emergono circa le modalità per consentire la decrittazione delle informazioni ai fini dell'accesso pubblico e della valutazione dei risultati (si pensi alle questioni potenzialmente sollevabili in punto di tipologia e funzionalità del relativo *software* utilizzato per il conteggio dei voti) come anche nella fase preliminare di individuazione delle categorie di dati da gestire su *blockchain* (ad esempio, il nominativo del votante oppure la creazione alternativa di un apposito ID anonimo, oltre all'espressione di voto relativa).

Complessa si presenta anche la fase di trasmissione del voto, che nei pochi millisecondi successivi alla sua espressione tramite, ad esempio, una app sullo smartphone, ben potrebbe essere intercettata mediante un *malware wi-fi* poco prima di essere gestita dai *server* che consentono il funzionamento della *blockchain*.

Alla manipolazione del voto, peraltro, si affiancano evidenti pericoli di *data breach*, laddove le informazioni personali dell'elettore – dati personali, recapiti, tendenza politica, indirizzo IP di connessione, sistema smartphone utilizzato – dovessero subire un accesso illegittimo (si pensi, ad esempio, agli elettori residenti o domiciliati al di fuori degli USA, come diplomatici, militari in missione, funzionari delle forze dell'ordine, che esporrebbero pertanto la loro condizione a terze parti).

La garanzia del diritto costituzionale di voto, quindi, almeno negli USA, non passa ancora definitivamente per la Rete.