Il voto in “via digitale”

Una sperimentazione di cui fare a meno.

Antonio Iacono

Con decreto del 9 luglio 2021 del ministro dell’Interno, di concerto con il ministro per l’Innovazione Tecnologica e la Transizione Digitale sono state approvate le linee guida per la “sperimentazione di modalità di espressione del voto in via digitale per le elezioni politiche ed europee e per i referendum limitata a modelli che garantiscano il concreto esercizio del diritto di voto degli italiani all’estero e degli elettori che, per motivi di lavoro, studio o cure mediche, si trovino in un comune di una regione diversa da quella del comune nelle cui liste elettorali risultano iscritti”.

Nel preambolo il decreto pone come primo elemento alla base dell’atto l’articolo 48 della Costituzione, il cui secondo comma, ricordiamolo, recita: “Il voto è personale ed eguale, libero e segreto. Il suo esercizio è dovere civico”.

Più avanti torneremo sui termini “personale” e “segreto”, adesso una breve premessa sulle sperimentazioni del voto elettronico.

L’Italia non è il primo e, temiamo, non sarà l’ultimo a sperimentare soluzioni di voto elettronico o, come cita il decreto, “voto in via digitale”.

Altri paesi, europei ed extraeuropei, negli anni hanno perseguito questa strada che, nella quasi totalità dei casi, si è rivelata irta di ostacoli portandoli ad abbandonare l’idea di affidarsi al digitale.

È successo in Norvegia (nel 2014), in Francia (nel 2017), in Finlandia (nel 2017), in Olanda (nel 2017).

In Germania, con la sentenza del 3 marzo 2009, il Tribunale costituzionale tedesco ha sottolineato che quella del voto elettronico è: “Una procedura di voto in cui l’elettore non può correttamente stabilire se il suo voto è conteggiato in modo genuino e incluso nel risultato finale al pari di tutti gli altri voti espressi, esclude dal controllo pubblico gli elementi centrali del procedimento e non soddisfa i requisiti costituzionali”.

E allora perché in Italia, dove questi concetti sono altrettanto cari alla dottrina e alla giurisprudenza, si vuole sperimentare questa modalità?

Può essere che in questo decennio l'innovazione tecnologica abbia fatto passi da gigante verso una sicurezza informatica pressoché assoluta?

La risposta è ovviamente no, tutt'altro. Il mondo del digitale è sempre meno sicuro. Truffe e manipolazioni sono all'ordine del giorno.

Torniamo al decreto e alle linee guida per sottolinearne solo alcuni aspetti.

Partiamo dall'articolo 2, comma 2.

"Il sistema di voto elettronico dovrebbe basarsi su una *web application*, conforme ai requisiti di usabilità e accessibilità previsti dalla legge, da utilizzare con qualsiasi dispositivo digitale (*smartphone, tablet, personal computer*) connesso alla rete *Internet* e dotato di uno dei *browser* più diffusi".

Così come nel voto tradizionale il "mezzo" per esprimere il voto è la matita "copiativa" ovvero quel particolare tipo di matita la cui traccia è indelebile, nel voto elettronico diventerebbe il browser (Google Chrome, Mozilla Firefox, Microsoft Edge, ecc.) contenuto nel dispositivo digitale.

I tecnici dei ministeri che hanno partecipato alla redazione delle linee guida sanno bene che i browser e i dispositivi digitali sono la causa numero uno dei problemi di sicurezza. Un browser non aggiornato, un dispositivo vecchiotto (o perfino, in alcuni casi, troppo recente) non assicura una corrispondenza tra quello che l'utente vede nello schermo del proprio dispositivo e ciò che il sito sta "trasmettendo" perché, magari, tra il dispositivo e il sito c'è "qualcuno" che interviene sui dati che vi transitano.

La rete Internet, infatti, non è un filo diretto dal dispositivo dell'utente al *cervellone* del ministero, ma una rete formata da una quantità smisurata di *nodi* e *connessioni* e che ogni singolo *pacchetto di dati* viene inviato letteralmente in giro per il mondo prima di giungere a destinazione. Seppure i dati siano in gran parte criptati, alcuni non lo sono (anzi non lo possono essere), quale ad esempio l'indirizzo IP (Internet Protocol) del mittente e del destinatario. Quindi un *provider* può, ad esempio, sapere benissimo se un utente si sta connettendo per votare.

Continuiamo con l'esame delle linee guida.

Il successivo articolo 3 al comma 2 recita: “Gli elettori dovrebbero essere identificati dal sistema di voto elettronico mediante l’identità digitale di cui all’articolo 64, comma 2-*quater*, del decreto legislativo n. 82 del 2005”, in sostanza con SPID. È vero che il CAD prevede anche carta di identità elettronica e la carta nazionale dei servizi per l’autenticazione, ma quest’ultima è ormai quasi abbandonata e la CIE è raramente utilizzata nei sistemi di identificazione.

Quindi SPID, quindi fornitori privati, esterni allo Stato. Questo significa che il fornitore SPID sa chi si sta autenticando per votare.

Articolo 4, comma 4: “Il voto espresso non deve essere riconducibile all’elettore. A tal fine, il sistema deve garantire che le informazioni sui votanti vengano separate da quelle sui voti espressi. Tali informazioni dunque vengono digitalmente ‘sigillate’ e rimangono del tutto indipendenti e separate. I voti sono e rimangono anonimi.”.

Comma del tutto pleonastico, è una ovvietà, un voto non anonimo sarebbe contro l’articolo 48 della Costituzione, da cui siamo partiti.

Articolo 4, comma 5: “Ogni elettore può votare una volta sola per ogni consultazione; deve quindi essere esclusa la possibilità di esprimere validamente il proprio suffragio due o più volte per la stessa consultazione”, ma premesso da: “Fatto salvo quanto previsto dall’articolo 1, comma 4”, che, invece, riporta: “Potrà essere valutata l’adozione di un processo di voto multiplo anche per affrontare il rischio di un’eventuale pressione esterna sugli elettori”. Valutata? Da chi, e come? Via software? Con algoritmo?

Articolo 5, secondo periodo del comma 1: “Il codice sorgente del sistema di voto elettronico dovrebbe essere pubblicato per consentire un’ampia verifica mediante mezzi indipendenti dal sistema stesso, anche al fine di garantire la massima confidenza nel sistema”.

Ecco, finalmente una frase che condividiamo, il codice sorgente deve essere pubblicato. Magari lo fosse il codice di ogni applicazione della pubblica amministrazione. In fondo è software che i cittadini, i contribuenti hanno pagato e pagano a ben caro prezzo.

Articolo 5, comma 4: “L’infrastruttura centrale del voto elettronico è gestita esclusivamente da personale autorizzato”.

Quindi stiamo affidando l’esito di una elezione politica ad una manciata di tecnici?

Anche in una elezione tradizionale possono avvenire brogli. In una sezione, in dieci ma certo non in tutte. Con un’infrastruttura centrale informatizzata potenzialmente sì.

Il codice sorgente del sistema di voto può anche essere pubblicato, ma chi ci assicura che il codice *in esecuzione* corrisponda a quello pubblicato?

Sviluppatori, sistemisti e tutti coloro che lavorano nel campo informatico sanno benissimo che il codice ormai è talmente complesso (alcuni software superano tranquillamente il milione di righe di istruzioni) che è impossibile accorgersi se qualcuna di queste *istruzioni* è stata modificata.

E per spostare voti da una lista all’altra, basta modificarne una.