Riflessioni sulla “indipendenza dal software” nei sistemi di e-voting (parte seconda)

Riprendiamo l’analisi critica del concetto di Sistema Indipendente dal Software proposto da Rivest **[1]** iniziato nell’articolo precedente andando a vedere come questa idea, che approfondisce il problema della fiducia dell’elettore sulla qualità del software che ne gestisce e registra il voto, abbia già diverse incarnazioni pratiche esistenti.

Esempi di sistemi indipendenti dal software

Rivest non si esime dal chiarire con degli esempi concreti il tema di “come” realizzare sistemi indipendenti dal software anzi riporta esempi di soluzioni esistenti che rientrano nella definizione.

Seppur sottolineando la vastità delle possibili soluzioni esistenti, Rivest si sofferma principalmente su due categorie principali: sistemi basati su un approccio VVPR (*Voter-Verifiable Paper Record*) – ovvero sistemi che consentono tramite un riconteggio la possibilità di rilevare e ricorreggere gli errori dovuti al software – e sistemi basati su crittografia.

L’esempio più importante di VVPR è il **sistema di voto a scansione ottica** utilizzato dalla maggior parte degli elettori nelle elezioni americane del 2006.

Il voto cartaceo è verificabile immediatamente dal votante perché l’elettore può attestare la precisione del voto prima

di essere inserito nello scanner ottico; la scheda elettorale serve quindi come traccia di controllo e può essere utilizzata negli audit post-elettorali. Un sistema elettronico di marcatura delle schede (EBM) può essere usato per registrare elettronicamente le scelte dell'elettore con un'interfaccia touch-screen che quindi stamperà una scheda elettorale certificabile da inserire nello scanner ottico. Una variante a questo sistema è il VVPAT (*Voter-Verifiable Paper Record Audit Trail)* simile a un DRE ma con una stampante e una logica aggiuntiva. Produce due registrazioni delle scelte dell'elettore, uno sul display touch-screen e uno su carta e l'elettore deve verificare che entrambi i record siano corretti prima di inviare il voto.

La categoria di sistemi basati su crittografia può fornire meccanismi di rilevamento per errori causati da modifiche del voto o errori del software **[2]**. L'approccio crittografico consente agli elettori di rilevare quando il loro voto è stato rappresentato in modo improprio e poter quindi richiedere una ri-votazione. Inoltre questi sistemi possono anche consentire a chiunque di rilevare quando i voti sono stati persi o cambiati, o quando il conteggio ufficiale è stato calcolato in modo errato e offrendo così un metodo per il recupero del voto. Rivest sottolinea nella sua analisi come la maggior parte dei sistemi di votazione crittografica proposti sono fortemente indipendenti dal software.

Problematiche dell'indipendenza dal software

La definizione di sistema indipendente dal software apre nuove problematiche tecniche a cui Rivest ci introduce:

- quali aspetti del sistema di voto lo rendono "indipendente dal software"?
- è solo l'hardware e il software, o include anche le procedure circostanti?

- un sistema di votazione è ancora indipendente dal software se non vengono eseguiti audit post-elettorali?

Come si evince dai temi elencati da Rivest, il tema non è specificatamente di natura informatica ma mostra ancora una volta come sia **fondamentale** che le questioni tecnologiche e legislative debbano oggi essere trattate **simbioticamente** allo scopo di garantire un'evoluzione che preservi la concretezza dei principi giuridici.

La risposta che Rivest ci da è che un sistema di votazione è indipendente dal software se, dopo aver preso in considerazione il suo software e il suo hardware, consenta l'uso di una qualsiasi procedura di verifica necessaria per determinare se il risultato elettorale sia accurato senza doversi fidare del fatto che il software del sistema di voto sia effettivamente del tutto corretto. Questo implica che il legislatore dovrebbe includere nelle procedure elettorali quelle azioni svolte dagli elettori, o nel caso di scansione ottica e VVPAT, dovrebbero includere procedure ufficiali di audit post-elettorali. Ci preme sottolineare che il legislatore dovrebbe assumere con serenità il fatto che il software non debba essere perfetto ma debba solo funzionare con una probabilità sufficientemente alta, in un ambiente ideale e dare la possibilità di verificare e individuare le anomalie.

Ad esempio, si consideri l'EBM che stampa un foglio di scansione ottica compilato. Alcuni votanti potrebbero non riesaminare il voto stampato. Eppure l'EBM sarebbe ancora un sistema indipendente dal software, poiché esiste una probabilità significativa che venga rilevato un comportamento scorretto del software da parte dell'EBM.

In questa nuova prospettiva **un ruolo importante lo riveste l'elettore** che, si assume, sia sufficientemente attento da rilevare i comportamenti scorretti. Questo comportamento virtuoso non può essere dato per scontato come anche Rivest

sottolinea: potrebbe essere necessario un aumento della formazione e della sensibilizzazione degli elettori.

Per chiarire ulteriormente la differenze tra un sistema indipendente dal software e uno dipendente dal software possiamo portare ad esempio i sistemi di voto tipo sondaggio (polling). Questi sistemi sono i più semplici da realizzare e primi che vengono in mente parlando di e-voting. I **sistemi di e-polling** purtroppo sono esempi di sistemi DRE (descritti inizialmente) e non sono quindi indipendenti dal software per costruzione, difatti non è possibile fare un audit per determinare la correttezza della registrazione del voto in modo indipendente dal software stesso. La loro dipendenza dal software porta gli eventi elettorali relativi immancabilmente al centro di polemiche ricorrenti poiché l'elettorato non attribuisce in modo uniforme la propria fiducia ai sistemi software.

Esempi in questo senso **in Italia** si possono trovare dell'esperimento del 2017 fatto in occasione del referendum regionale sull'indipendenza amministrativa della Lombardia o più recentemente sulle votazioni sulla piattaforma Rousseau interne al Movimento 5 Stelle. In entrambi i casi, l'utilizzo di sistemi non indipendenti dal software e le relative complessità tecniche hanno compromesso il valore percepito da parte dell'elettorato. L'applicazione del concetto di Indipendenza del Software potrebbe in questi scenari preservare il valore culturale e politico di iniziative simili di e-democracy evitando ai cittadini la necessità di atteggiamenti fideistici e garantire il valore democratico delle consultazioni evitando ai rappresentanti politici che scelgono la via dell'innovazione per avvicinare la democrazia diretta e quella rappresentativa, un'impossibile difesa del risultato ottenuto.

Conclusione

La riflessione con cui vogliamo chiudere questa revisione critica all'articolo di Rivest è che, sebbene l'articolo originale sia 2008 (nel mondo dell'informatica, un'era fa) il suo contenuto resta **fortemente attuale**. Rivest dimostra che fin dal 2008 la tecnologia per una corretta implementazione dell'e-voting esiste e che ci sono i presupposti per poter analizzare, studiare e risolvere il problema. Tuttavia è necessario avvalersi di professionisti seri che sappiano di cosa si parli, che abbiano competenze trasversali nel campo dell'informatica e del diritto, che lavorino gomito a gomito in team di esperti di cyber security, di blockchain, di software, di application security e di ingegneria del software per la progettazione dei migliori modelli.

Tutto questo merita una riflessione a diversi livelli e sarà nostra cura tornare a stimolare il dibattito sul tema, magari in articoli successivi.

Note:

[1] Ronald L Rivest, *On the notion of 'software independence' in voting systems*. Published: 06 August 2008 – https://doi.org/10.1098/rsta.2008.0149.

[2] Adida 2006, Chaum 2004, Chaum et al. 2004, Karloff et al., 2005, Neff 2004, Ryan & Peacock 2005, Ryan & Schneider 2006.

Articolo a cura di **Michelangelo De Bonis** e **Matteo De Simone**

https://www.ictsecuritymagazine.com/articoli/riflessioni-sulla-indipendenza-dal-software-nei-sistemi-di-e-voting-parte-seconda/