

Il Pedante

Assange ci aveva judo

Pubblicato il Ven 3 novembre 2017, 11:45 su ilpedante.info

Ultimo aggiornamento il Mar 16 aprile 2024, 15:15

L'[articolo precedente](#) sui pericoli del voto elettronico ha suscitato le obiezioni di alcuni lettori che mi offrono in questa appendice lo spunto per integrare e completare la fenomenologia lì intrapresa.

Molti di quei lettori hanno parlato di tecnologia **blockchain** per contestare le mie analisi sull'insicurezza intrinseca delle procedure informatiche applicate al voto e, in subordine, ad altri ambiti critici come denaro, salute, comunicazioni riservate. La blockchain è un sistema di replicazione e distribuzione di una base di dati corredata da un certificato elettronico non falsificabile che ne attesta la coerenza in un dato momento. Le informazioni contenute in un database protetto da blockchain non possono essere alterate dai non aventi diritto, perché ciò determinerebbe l'incoerenza del set con gli altri esemplari, e quindi la sua falsificazione. I database protetti sono criptati, sicché risultano illeggibili a chi non ne è proprietario o utente autorizzato.

Ora, in che modo questa ingegnosa tecnologia può rendere il voto elettronico sicuro almeno tanto quanto il cartaceo? Purtroppo, **in nessun modo**. Innanzitutto perché si applica alla *conservazione* dei dati, non alla loro *acquisizione*, cioè non al problema sollevato nell'articolo di garantire la coerenza dell'input (il dito che tocca «sì» sul tablet) con l'output (il tablet che scrive «sì» nel database). Per gli stessi motivi, non può nemmeno certificare la bontà del codice installato sui dispositivi.

Un [problema irrisolvibile a monte](#), che diventa drammatico nella sciagurata variante del voto online, è che con i sistemi elettronici di voto **non si possono soddisfare contemporaneamente i requisiti dell'anonimato e della verificabilità del voto**. Se si tutela l'anonimato come nell'implementazione primitiva del referendum lombardo, l'elettore non ha la possibilità di verificare che il suo voto sia stato registrato correttamente, sicché deve fidarsi di chi gestisce il sistema. Se invece si certifica elettronicamente il voto collegandolo all'identità digitale di chi lo ha espresso per consentirgli di verificarlo (e quindi anche di mostrarlo a chi glielo ha eventualmente estorto o comprato), occorre comunque fidarsi di chi assegna le chiavi del certificato,

che non le registri in modo da risalire ai votanti o, mancando i controlli fisici (voto online, postale), addirittura non le utilizzi in loro vece. In ogni caso, il requisito di verificabilità sarebbe soddisfatto solo in misura campionaria.

Come si svilupperà meglio nel seguito, in generale ogni singola vulnerabilità dei sistemi informatizzati (backdoor, manipolazioni di insider o terzi, bachi, blackout delle reti, malfunzionamenti ecc.) è una vulnerabilità *di sistema* che si estende a larghi gruppi di utenti (multicast) o a tutti (broadcast), laddove le vulnerabilità di una procedura fisica, certamente esistenti e quand'anche più numerose, colpiscono solo i nodi del sistema dove ci si è effettivamente assunti il costo di sfruttarle. Come una leva di Archimede, una sola manipolazione elettronica produce effetti più estesi di migliaia di manipolazioni fisiche. Tutto ciò limitando il discorso agli illeciti. Se si aggiungono gli abusi *legali* e ci si allarga agli altri ambiti toccati nel dibattito, quali garanzie può opporre una procedura certificata a una requisizione di denaro elettronico via [bail in](#), al blocco di un conto corrente, allo [spionaggio di stato](#), all'[hackeraggio di uno smartphone o di una televisione](#)?

Prima di procedere oltre è però importante però fissare un punto: che queste obiezioni e controobiezioni sono sì apparentemente tecniche, mahanno poco o nulla di tecnico. Il criterio tecnico e i suoi rivoli argomentativi si giocano infatti negli spazi ristretti del metodo che le informa. Occorre quindi prima circoscrivere quel metodo, denunciarne il pericolo e analizzare i moventi di chi rinuncia a difendersene. Procederemo per punti, assegnando a ciascun fenomeno un nome.

Tecnicorum. Non è un caso che spesso (non sempre) le obiezioni di tenore tecnico provenissero dai lettori tecnicamente meno preparati, laddove l'opinione degli studiosi sul punto è [piuttosto tombale](#). Il paradigma tecnocratico si legittima agli occhi di chi lo subisce alimentando l'illusione che una procedura o un sistema di regole possano effettivamente sterilizzare i danni dell'incompetenza e dell'avidità degli umani. È la fede nel «pilota automatico», nello strumento che si fa garante del fine. La complessità è funzionale al paradigma nella misura in cui diluisce e occulta nei meandri della tecnica gli umanissimi appetiti degli esseri umani che iniziano, gestiscono e normano quelle procedure.

[Su questo blog](#) si è ad esempio mostrato come le regolazioni bizantine del mercato energetico conducano banalmente a soppiantare il monopolio pubblico con un monopolio privato. Così gli infiniti paragrafi e comma dei trattati di libero scambio (TTIP, CETA) mascherano e proteggono l'avidità dei mercati più forti, la raffinatezza degli strumenti finanziari dissimula l'usura e i parametri del rating e dello spread fanno apparire le politiche a beneficio dei ricchi come il prodotto di complicate valutazioni economiche.

Illusione di controllo. L'abitudine alla democrazia produce la sua illusione. Se la rete internet su cui scrivo è stata data alle masse trent'anni dopo la sua invenzione, è ragionevole almeno sospettare che le tutele tecnologiche che ci scaldano il cuore

siano in ritardo di altri trent'anni. Che, ad esempio, la crittografia a numeri primi possa già risolversi e manipolarsi con calcolatori più potenti di quelli in commercio, o che i processori più diffusi possano registrare e inviare a terzi gli input dei dispositivi. Qualcuno obietta, sollevato, che il vantaggio tecnologico sarebbe comunque appannaggio delle agenzie dei governi. Ma se anche fosse vero - e chi scrive ne dubita - *è proprio attraverso le elezioni* che i governi, e quindi le loro agenzie, legittimano e alimentano i loro poteri.

In generale, il fatto di scorrazzare più o meno liberamente su reti e calcolatori ci dà la sensazione di esserne i padroni. Ma non è così.

Questismo. Un problema di metodo ancora più serio è che nelle elezioni lombarde e nelle tante già celebrate con il voto elettronico (la sola Smartmatic ne dichiara [più di 3500](#)) non si son mai utilizzate, salvo poche e parziali sperimentazioni, le tecnologie magnificate dai suoi difensori. Sicché l'immaginazione di un sistema diverso *che non esiste* anestetizza l'opposizione a ciò *che esiste*, l'illusione di imporre *domani* ai decisori l'impiego di tecnologie «sicure» lascia *oggi* il campo libero a quei decisori, di impiegare tecnologie insicure e pericolose. Di questismo [ci siamo occupati](#) in passato per esporre le contraddizioni dei sostenitori «critici» dell'Unione Europea, ma le sue applicazioni sono evidentemente più ampie e identificano il dramma di una società malata di simboli dove i diritti dell'involucro e della narrazione prevalgono sui contenuti, il *poter essere* sull'*essere* da cui devono principiare le analisi.

Booleismo o indifferenza quantitativa. Nell'articolo precedente si è osservato in chiusura come nella foga della digitalizzazione covi il sogno di un'umanità confusa di disumanizzarsi per soddisfare gli algoritmi economici e sociali a cui è richiamata. Corollario di questa deriva è il vizio analitico di anteporre il *quid* al *quantum*, cioè il pensiero binario (esiste/non esiste) proprio delle idee e, appunto, dei computer, a quello quantitativo (più/meno) proprio degli oggetti reali. Sicché il rischio centralizzato e massificato di brogli elettronici non preoccupa, perché «si può imbrogliare anche con le schede cartacee», né preoccupano i rischi di tracciamento e requisizione del denaro elettronico, perché «con un mandato possono già aprirti la cassetta di sicurezza». La mera esistenza del fenomeno (*quid*) rende futile la quantificazione (*quantum*) della sua intensità e probabilità, appiattendolo la sproporzione che distingue *in punto di sostanza* la difficoltà di un intervento fisico distribuito (per quanto sì, teoricamente possibile) dalla semplicità di un'azione istantanea, tecnologicamente assistita e dalle conseguenze seriali.

L'ultima aporia ci porta al problema centrale della nostra appendice: la **concentrazione del potere** come parametro - quindi *non* fenomeno, ma parametro *misurabile* - della libertà e sicurezza dei membri di una comunità governata. Il problema fa il paio, e in certa misura vi si sovrappone, con quello della concentrazione delle ricchezze e dei conseguenti squilibri sociali. È facile intuire che

un potere è tanto più arbitrario ed esclusivo delle libertà altrui quanto più è **centralizzato**, intendendosi qui la centralizzazione non già in termini gerarchici e ordinamentali (ad es. nella dialettica di Stato centrale vs federale), ma strettamente numerici e quantitativi, cioè di *quante* persone esercitino un potere, su *quante* persone e con *quanta* facilità. In pseudoformula:

Dove:

- $Conc_p$ è la concentrazione di un potere p all'interno di un gruppo a ,
- P_a è la percentuale di persone appartenenti al gruppo a che subiscono il potere p ,
- D è la somma dei decisori ed esecutori necessari all'esercizio del potere p (dimensione della catena decisionale),
- C è il costo necessario all'esercizio del potere p : costi economici diretti, numero di azioni richieste, difficoltà fisiche e logistiche, eventuali rischi legali ecc.

In un totalitarismo teorico, un'unica persona ($D = 1$) eserciterebbe il potere p su tutti i membri di una comunità ($P_a = 1$) senza sostenere alcun costo ($C \rightarrow 0^+$), ad esempio pigiando il tasto di un terminale.

L'informatizzazione dei processi è sempre, in sé, un fattore di accrescimento della concentrazione ($Conc_p$). Nel caso del voto elettronico un manipolo di sviluppatori istruiti da un vertice ($D < 10$) può scrivere, compilare e installare un codice maligno sui server o dispositivi di voto ($P_a = 1$) con un differenziale di costo impercettibile rispetto a un'operatività «onesta» ($\Delta C \rightarrow 0^+$), laddove per ottenere lo stesso effetto con sistemi tradizionali sarebbe necessario corrompere singolarmente (ΔC nell'ordine dei milioni, o miliardi) tutti gli scrutatori e presidenti di seggio (D nell'ordine delle centinaia di migliaia). Non serve essere matematici per capire che i due risultati si rapportano nell'ordine delle **centinaia di miliardi**: a tanto ammonta la moltiplicazione del rischio collegata alla seconda opzione, che [qualcuno](#) ha il coraggio di definire «il futuro» della democrazia. Risultati analoghi si otterrebbero applicando la formula al potere di requisizione del denaro elettronico tramite canali telematici capillari e rapportando il risultato all'investigazione, ricerca e sequestro fisico di milioni di casseforti.

L'idea che la **disseminazione delle responsabilità e degli ostacoli all'esercizio di un potere garantiscano la sicurezza e i diritti** di tutti è in fondo - e non fortuitamente - la stessa che ispira la tecnologia blockchain, diffusa e computazionalmente dispendiosa. Ma più e prima ancora è un **principio fondante della democrazia**, la quale allarga la base dei poteri intrecciando «pesi e contrappesi», organi di vigilanza,

collegi giudicanti e legislativi, commissioni, articolate gerarchie di comando ecc. e coinvolgendo periodicamente l'intera cittadinanza nella nomina di chi la amministra. Questa ragnatela istituzionale mantiene alti i valori delle variabili D (numero dei decisori) e C (costi delle decisioni), cioè del denominatore, limitando i rischi della concentrazione.

Non è assolutamente un caso che in anni recenti queste due garanzie - la diffusione dei poteri decisionali e il loro costo - siano esplicitamente demonizzate dai teorici, commentatori e protagonisti più accreditati e vocali del «riformismo» politico. Né che seguano gli appelli a «tagliare i costi della politica», rimuovere «lacci e lacciuoli», diminuire i parlamentari, sopprimere organi politici come le province e il Senato, snellire ulteriormente i processi legislativi, «disintermediare» i rapporti di lavoro ecc. Tutto serve a ridimensionare il denominatore e, quindi, a consegnare più poteri a un numero più ristretto di decisori. Serve a **trasformare la democrazia in oligarchia**.

La natura intrinsecamente concentratrice della digitalizzazione si presta ottimamente a questo progetto sicché, pur riconoscendone e valorizzandone le opportunità, è urgente rifiutarne le seduzioni qualora i benefici conseguibili non siano dimostrati e ampiamente eccedenti il rischio: come *non* è appunto il caso del voto elettronico. Più che volerla salvare a tutti i costi per amore del futuro in sé, occorre cogliere nella corsa all'elettrone una valenza *politica* che non è invece sfuggita a chi se ne è intestato il governo. Se alla presidenza della più importante azienda di e-voting siede il braccio destro di George Soros non è perché, in quel momento, **Assange ci aveva judo**.

Ringrazio sentitamente l'amico [Minuteman](#) per la peer review della parte tecnica.