CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Scientifico

BLOCKCHAIN, SMART CONTRACT E VOTO ELETTRONICO: PROFILI COSTITUZIONALI E QUESTIONI APERTE SULLA SEGRETEZZA DELL´ART. 48 COST.

Il contributo analizza, in prospettiva integrata costituzionale e tecnologica, l?impiego di blockchain e smart contract nel voto elettronico, con particolare riferimento alla segretezza ex art. 48 Cost. L?articolo evidenzia le tensioni tra permanenza e trasparenza del dato e l?esigenza di non ricostruibilit? della scelta, approfondendo il tema della coercizione (receipt-freeness), dei metadati e della sicurezza end-to-end (anche alla luce del caso Voatz). Sono inoltre considerati gli standard del Consiglio d?Europa e dell?OSCE/ODIHR, nonch? i profili comparati. In chiave prudenziale, si prospetta un uso selettivo della tecnologia in fasi non sensibili del procedimento elettorale.

di **Salvatore Stanizzi**
IUS/08 - DIRITTO COSTITUZIONALE
Estratto dal n. 4/2026 - ISSN 2532-9871

Direttore responsabile
Alessio Giaquinto

Pubblicato, Mercoledì 15 Aprile 2026

CamminoDiritto.it
ISSN 2532-9871

Abstract ENG

This article provides an integrated constitutional and technological assessment of blockchain and smart contracts in electronic voting, focusing on the secrecy requirement under Article 48 of the Italian Constitution. It highlights the structural tension between data permanence and transparency, on the one hand, and the constitutional need for absolute non-traceability, on the other. The analysis addresses coercion-related concerns (receipt-freeness), metadata risks, and end-to-end security issues (including the Voatz case), also considering Council of Europe and OSCE/ODIHR standards as well as comparative perspectives. Adopting a cautious approach, the article suggests a selective use of such technologies in non-sensitive stages of the electoral process.

Sommario: 1. Introduzione; 2. L'art. 48 Cost. e la segretezza del voto tra libertà, non dimostrabilità e contesto di esercizio; 3. Blockchain e voto elettronico: struttura tecnica e implicazioni giuridiche; 4. Il caso Voatz e la vulerabilità dell'infrastruttura: oltre la blockchain; 5. Trasparenza, verificabilità e segretezza: un equilibrio problematico; 6. Esperienze comparate e standard internazionali: un approccio prudente al voto elettronico; 7. Segretezza del voto e limiti della traducibilità tecnica: verso una lettura costituzionalmente orientata; 8. Conclusioni.

1. Introduzione

La possibilità di integrare tecnologie basate su blockchain e smart contract nei processi elettorali costituisce oggi uno dei nodi più delicati nel rapporto tra innovazione tecnologica e diritto costituzionale. In particolare, il voto elettronico – soprattutto nelle sue forme più avanzate e decentralizzate – viene frequentemente presentato come uno strumento idoneo a rafforzare l'integrità del processo elettorale, ridurre il rischio di manipolazioni e accrescere la fiducia dei cittadini nelle istituzioni democratiche. Tali promesse si fondano, in larga misura, sulle caratteristiche tecniche dei registri distribuiti, quali l'immutabilità dei dati, la trasparenza delle operazioni e la possibilità di verifica diffusa delle transazioni[1].

Tuttavia, nel quadro costituzionale italiano, ogni riflessione sul voto non può che confrontarsi con un nucleo di principi che assumono carattere strutturale e non comprimibile. L'art. 48 Cost. stabilisce infatti che il voto è personale, eguale, libero e segreto, delineando un insieme di garanzie che non si esauriscono nella mera regolarità procedurale, ma attengono alla stessa legittimazione democratica del potere politico[2]. In particolare, la segretezza del voto non rappresenta soltanto una tutela della sfera privata dell'elettore, ma costituisce una condizione essenziale per evitare forme di pressione,

CamminoDiritto.it
ISSN 2532-9871

controllo o ritorsione, assicurando che la scelta politica possa formarsi ed esprimersi in piena autonomia[3].

In questa prospettiva, la segretezza non deve essere intesa in senso meramente formale, come semplice non conoscibilità immediata della scelta, ma come impossibilità strutturale di ricostruire ex post il collegamento tra elettore e voto espresso. Tale dimensione sostanziale emerge con particolare evidenza nelle riflessioni sviluppate a livello europeo e internazionale, ove la segretezza è costantemente qualificata come elemento imprescindibile delle elezioni democratiche[4]. Non a caso, la Commissione di Venezia ha incluso la segretezza tra i principi fondamentali del diritto elettorale, sottolineando come essa debba essere garantita non solo sul piano normativo, ma anche attraverso adeguate soluzioni tecniche e organizzative[5].

Il problema assume contorni ancora più complessi nel caso del voto elettronico remoto, ossia non esercitato in un ambiente "presidiato" quale il seggio elettorale. In tali ipotesi, la letteratura ha evidenziato come la segretezza possa risultare compromessa non soltanto da vulnerabilità tecniche, ma anche da fattori esterni, quali la coercizione o l'influenza indebita, che il sistema non è in grado di prevenire efficacemente[6]. Questo profilo, già emerso con riferimento al voto per corrispondenza, si ripropone con maggiore intensità nei sistemi digitali, nei quali l'atto di voto si colloca al di fuori di uno spazio istituzionalmente controllato.

A ciò si aggiunge un ulteriore elemento di tensione: mentre la logica costituzionale della segretezza richiede la non tracciabilità del voto, le tecnologie blockchain sono progettate per garantire, al contrario, la registrazione permanente e verificabile delle operazioni. Come evidenziato nella letteratura tecnico-giuridica, tale tensione non è meramente teorica, ma si traduce in difficoltà concrete nel conciliare verificabilità e anonimato, soprattutto in contesti caratterizzati da elevata complessità infrastrutturale[7].

Alla luce di tali considerazioni, il presente contributo si propone di analizzare in chiave integrata i profili costituzionali e tecnologici del voto elettronico basato su blockchain, con particolare attenzione al principio di segretezza. L'obiettivo non è quello di formulare giudizi definitivi sulla compatibilità di tali strumenti con il quadro costituzionale, ma piuttosto di mettere in luce le principali criticità e le questioni ancora aperte, anche alla luce delle esperienze comparate e delle più recenti analisi in materia di sicurezza dei sistemi di voto elettronico[8].

2. L'art. 48 Cost. e la segretezza del voto tra libertà, non dimostrabilità e contesto di esercizio

CamminoDiritto.it
ISSN 2532-9871

La segretezza del voto, nel sistema costituzionale italiano, non può essere ridotta a una garanzia meramente individuale o ad un riflesso del diritto alla riservatezza. Essa svolge una funzione eminentemente pubblicistica, in quanto protegge il libero formarsi della volontà politica dell'elettore e, al tempo stesso, preserva l'autenticità della competizione democratica. L'art. 48 Cost., nel qualificare il voto come personale, eguale, libero e segreto, non delinea infatti una serie di attributi eterogenei, ma individua un complesso unitario di garanzie che si sostengono reciprocamente: la segretezza, in particolare, opera come condizione della libertà, poiché rende più difficile – e idealmente impossibile – ogni forma di pressione, controllo o verifica esterna della scelta espressa[9].

In questa prospettiva, la segretezza non deve essere intesa soltanto come non conoscibilità immediata del contenuto del voto, ma come non dimostrabilità della preferenza politica. Il punto è decisivo: un voto può dirsi realmente segreto non solo quando terzi non conoscano la scelta dell'elettore, ma quando l'elettore stesso non sia in condizione di fornirne prova in modo attendibile. È precisamente in questa direzione che si sviluppano, anche sul piano comparato e tecnologico, le categorie della receipt-freeness e della coercion resistance, che rappresentano una traduzione tecnico-funzionale di una preoccupazione ben nota al costituzionalismo democratico[10].

A tale riguardo, merita un approfondimento ulteriore il tema del voto non presidiato, cui il revisore opportunamente richiama l'attenzione. La segretezza del voto, infatti, non dipende soltanto dalla struttura della procedura, ma anche dal contesto concreto in cui la volontà elettorale si forma ed è espressa. Nel voto esercitato all'interno del seggio, l'ordinamento predispone un ambiente istituzionalmente protetto, nel quale la cabina elettorale, la ritualità delle operazioni e il controllo pubblico delle fasi esterne allo scrutinio costituiscono elementi di presidio della libertà dell'elettore. Diversamente, nel voto remoto – e dunque in una forma di voto non presidiato – tali garanzie ambientali tendono a indebolirsi, perché l'atto di voto si sposta in uno spazio privato, sottratto al controllo dell'autorità pubblica e potenzialmente esposto a pressioni familiari, economiche o sociali[11].

Sotto questo profilo, il problema non nasce con la blockchain. Una questione analoga, sia pure in forma diversa, si pone da tempo anche con riferimento al voto per corrispondenza, nel quale l'espressione del voto avviene al di fuori di uno spazio protetto e istituzionalmente sorvegliato. Proprio tale parallelismo consente di chiarire che il nodo giuridico centrale non è esclusivamente la sicurezza della piattaforma tecnologica, ma il rapporto tra libertà sostanziale del voto e contesto materiale del suo esercizio. In altri termini, la segretezza può risultare vulnerata non solo quando il voto sia tecnicamente ricostruibile, ma anche quando l'elettore sia chiamato a votare in una situazione nella quale l'autonomia della scelta non è adeguatamente garantita[12].

CamminoDiritto.it
ISSN 2532-9871

Questa impostazione trova conferma sia nella riflessione sovranazionale sia nella più recente dottrina italiana sul voto elettronico. La Commissione di Venezia include la segretezza tra i principi fondamentali delle elezioni democratiche e insiste sul fatto che essa debba essere assicurata in modo effettivo, non solo astratto[13]. In modo particolarmente utile per il nostro discorso, Caterina e Giannelli, in un contributo del 2021 interamente dedicato alla valutazione costituzionale del voto elettronico e del voto con blockchain, sottolineano come il parametro della segretezza non possa essere letto in termini puramente tecnici, ma debba essere collegato ai contesti concreti di esercizio del voto e al rischio che la digitalizzazione, specie se remota, alteri il bilanciamento fra libertà, uguaglianza e affidabilità del procedimento[14]. In questa direzione si colloca anche una parte della dottrina italiana più recente, che ha esaminato criticamente il voto elettronico – e in particolare il home vote – alla luce dei principi di libertà e segretezza, mettendo in luce i rischi specifici connessi al venir meno del presidio del seggio e alle forme di voto da remoto[15].

Ne consegue che il confronto con il voto elettronico – e, a maggior ragione, con il voto su blockchain – non può essere impostato esclusivamente in termini di efficienza, velocità o integrità del dato. Prima ancora di interrogarsi sulla sicurezza dell'infrastruttura, occorre verificare se il modello tecnologico prescelto sia compatibile con una nozione costituzionale di segretezza che non riguarda soltanto il "come" il voto viene registrato, ma anche il "dove" e il "in quali condizioni" esso viene espresso. È su questo terreno che il tema della segretezza mostra la sua natura più profonda: non semplice requisito formale, ma garanzia della libertà politica nel suo momento più vulnerabile.

3. Blockchain e voto elettronico: struttura tecnica e implicazioni giuridiche

L'interesse per l'impiego della blockchain nei sistemi di voto elettronico deriva principalmente dalle caratteristiche strutturali di tale tecnologia, che appare, almeno in una prima lettura, idonea a garantire elevati livelli di integrità, trasparenza e verificabilità del dato elettorale. In un registro distribuito, infatti, ogni operazione viene validata attraverso meccanismi di consenso e successivamente inserita in una catena di blocchi crittograficamente collegati, rendendo estremamente difficile la modifica retroattiva delle informazioni registrate[16]. Questo assetto ha indotto parte della letteratura a ritenere che la blockchain possa offrire una risposta efficace ai tradizionali problemi di sicurezza e fiducia che affliggono i sistemi di voto elettronico.

Tuttavia, una più attenta analisi mostra come tali caratteristiche, lungi dal risolvere automaticamente le criticità del voto digitale, introducano nuove tensioni rispetto ai principi costituzionali che regolano il suffragio. In particolare, la trasparenza e la tracciabilità delle operazioni – elementi centrali nella logica dei registri distribuiti – si

CamminoDiritto.it
ISSN 2532-9871

pongono in rapporto problematico con il requisito della segretezza del voto, soprattutto se intesa nella sua dimensione sostanziale di non ricostruibilità. La possibilità che dati, metadati o correlazioni indirette consentano, anche ex post, di risalire all'identità dell'elettore o di restringere significativamente il campo delle possibili attribuzioni costituisce un rischio che non può essere trascurato[17].

In questo senso, la letteratura tecnico-giuridica più recente ha evidenziato come i sistemi di blockchain voting non solo non eliminino i problemi già noti dell'e-voting, ma possano addirittura amplificarli. Park, Specter, Narula e Rivest sottolineano come l'introduzione della blockchain non incida sulle vulnerabilità fondamentali dei sistemi di voto remoto, tra cui la sicurezza dei dispositivi dell'elettore, la gestione delle chiavi crittografiche e la possibilità di attacchi lungo l'intera infrastruttura[18]. In termini analoghi, il rapporto delle National Academies statunitensi evidenzia come il voto elettronico remoto comporti rischi sistemici difficilmente mitigabili, raccomandando un approccio estremamente prudente, soprattutto quando siano coinvolte tecnologie con elevata complessità operativa[19].

Un ulteriore profilo critico riguarda il rapporto tra verificabilità e anonimato. I sistemi di voto basati su blockchain sono spesso presentati come end-to-end verifiable, ossia come sistemi nei quali ogni elettore può verificare che il proprio voto sia stato correttamente registrato e conteggiato. Tuttavia, come evidenziato già nei lavori pionieristici di Chaum e, successivamente, di Benaloh, la verificabilità individuale del voto deve essere progettata in modo tale da non trasformarsi in una forma di "ricevuta" utilizzabile per dimostrare la scelta effettuata[20]. In caso contrario, il sistema rischia di compromettere proprio quella non dimostrabilità che costituisce uno degli elementi essenziali della segretezza del voto.

Da questo punto di vista, il problema non è soltanto tecnico, ma profondamente giuridico. La tensione tra verificabilità e segretezza riflette infatti due esigenze entrambe fondamentali: da un lato, garantire la correttezza e l'affidabilità del risultato elettorale; dall'altro, preservare la libertà dell'elettore. Il punto critico è che tali esigenze non sono sempre pienamente conciliabili, soprattutto quando il sistema tecnologico è progettato secondo logiche di trasparenza radicale e di persistenza dei dati, come avviene nella blockchain[21].

Ne consegue che l'introduzione di tali tecnologie nel contesto elettorale non può essere valutata esclusivamente sulla base delle loro prestazioni tecniche, ma richiede un'analisi più ampia, che tenga conto delle implicazioni costituzionali e delle condizioni concrete di utilizzo. In particolare, appare necessario interrogarsi su come le caratteristiche intrinseche della blockchain possano essere adattate – o eventualmente limitate – per risultare compatibili con un modello di voto che, per definizione, richiede l'opacità del

CamminoDiritto.it
ISSN 2532-9871

contenuto della scelta individuale.

4. Il caso Voatz e le vulnerabilità dell'infrastruttura: oltre la blockchain

L'analisi delle implicazioni costituzionali del voto elettronico basato su blockchain non può prescindere dall'esame di casi concreti nei quali tali soluzioni sono state effettivamente sperimentate. Tra questi, il sistema Voatz rappresenta uno degli esempi più discussi, in quanto frequentemente richiamato come modello di applicazione della blockchain al voto remoto. L'esperienza Voatz è stata utilizzata, in particolare negli Stati Uniti, per consentire il voto a distanza in contesti specifici, come quello del personale militare all'estero. Tuttavia, proprio l'analisi tecnica di tale sistema ha evidenziato criticità rilevanti, che mettono in discussione l'affidabilità complessiva dell'approccio.

In uno studio ampiamente citato, Specter, Koppel e Weitzner hanno sottoposto il sistema Voatz a un'approfondita analisi di sicurezza, evidenziando una serie di vulnerabilità lungo l'intera infrastruttura, che vanno ben oltre la dimensione strettamente "blockchain"[22]. In particolare, gli autori hanno dimostrato come un attaccante con capacità relativamente limitate potesse compromettere il dispositivo dell'elettore, alterare il voto espresso o intercettare informazioni sensibili, senza che tali manipolazioni risultassero necessariamente rilevabili dal sistema. Ciò conferma come la sicurezza del voto elettronico non dipenda unicamente dall'integrità del registro finale, ma dall'affidabilità dell'intero ecosistema tecnologico, che include dispositivi, applicazioni, reti e sistemi di autenticazione.

Il caso Voatz è particolarmente significativo perché consente di chiarire un equivoco ricorrente nel dibattito pubblico: l'idea secondo cui l'adozione della blockchain sarebbe di per sé sufficiente a garantire la sicurezza e la trasparenza del voto. In realtà, come evidenziato dalla letteratura tecnica, la blockchain interviene in una fase specifica del processo – quella della registrazione e della conservazione del dato – ma non è in grado di risolvere le vulnerabilità che si collocano a monte, ossia nel momento in cui il voto viene espresso e trasmesso[23]. In altri termini, se l'input del sistema è compromesso, l'immutabilità del registro non solo non costituisce una garanzia, ma rischia di cristallizzare un dato alterato.

Tale profilo assume particolare rilevanza anche sul piano costituzionale. Se, infatti, la segretezza del voto deve essere intesa come impossibilità di ricostruire la scelta individuale, le vulnerabilità dell'infrastruttura possono incidere non solo sull'integrità del risultato, ma anche sulla riservatezza del processo. Un sistema che consenta l'intercettazione dei dati o l'accesso non autorizzato ai dispositivi dell'elettore può determinare una compromissione indiretta della segretezza, anche in assenza di una

CamminoDiritto.it
ISSN 2532-9871

violazione esplicita del registro finale[24].

Inoltre, il caso Voatz evidenzia un ulteriore elemento di criticità, già emerso nella riflessione sul voto remoto: la difficoltà di garantire che l'elettore operi in condizioni di libertà effettiva. Il fatto che il voto sia espresso tramite un dispositivo personale, in un ambiente non controllato, rende più complesso escludere forme di coercizione, pressione o compravendita del voto. In tale contesto, la tecnologia non è in grado di sostituire le garanzie ambientali tipiche del seggio elettorale, che svolgono una funzione essenziale nella tutela della libertà e della segretezza del voto[25].

Queste considerazioni trovano conferma anche in ulteriori analisi tecniche e istituzionali, che sottolineano come i sistemi di voto elettronico remoto presentino rischi strutturali difficilmente eliminabili. Le linee guida del National Institute of Standards and Technology, così come i documenti dell'OSCE/ODIHR e del Consiglio d'Europa, insistono sulla necessità di un approccio estremamente prudente, evidenziando come la sicurezza del voto non possa essere valutata isolatamente, ma debba essere considerata nel contesto più ampio dell'intero processo elettorale[26].

In definitiva, il caso Voatz dimostra come il ricorso alla blockchain non consenta di superare le criticità fondamentali del voto elettronico remoto e, anzi, rischi di spostare l'attenzione su un segmento limitato del sistema, trascurando le vulnerabilità più rilevanti. Ne deriva l'esigenza di un'analisi che non si limiti alla dimensione tecnologica, ma che tenga conto dell'interazione tra infrastruttura digitale, contesto di esercizio del voto e principi costituzionali, in particolare con riferimento alla segretezza e alla libertà del suffragio.

5. Trasparenza, verificabilità e segretezza: un equilibrio problematico

Il dibattito sul voto elettronico basato su blockchain si concentra, in larga misura, sulla possibilità di coniugare due esigenze fondamentali: da un lato, la trasparenza e la verificabilità del processo elettorale; dall'altro, la tutela della segretezza del voto. Tali esigenze, considerate isolatamente, appaiono coerenti con i principi democratici. Tuttavia, la loro combinazione all'interno di un medesimo sistema tecnologico pone problemi non trascurabili, che emergono con particolare evidenza nel contesto delle architetture distribuite[27].

La trasparenza è tradizionalmente intesa come condizione di affidabilità del processo elettorale: la possibilità di controllare le operazioni, verificare la correttezza dello scrutinio e accertare l'assenza di manipolazioni costituisce un elemento essenziale per la fiducia pubblica. In questa prospettiva, i sistemi basati su blockchain sembrano offrire un

CamminoDiritto.it
ISSN 2532-9871

vantaggio significativo, in quanto consentono la registrazione pubblica e immutabile delle operazioni. Tuttavia, tale modello di trasparenza radicale entra in tensione con il principio della segretezza, soprattutto quando la verificabilità si estende fino al livello individuale del voto[28].

Il nodo centrale emerge nei sistemi end-to-end verifiable, nei quali l'elettore può verificare che il proprio voto sia stato correttamente registrato e conteggiato. Se tale caratteristica rafforza la fiducia nel sistema, essa rischia al tempo stesso di introdurre una forma di tracciabilità incompatibile con la segretezza, qualora consenta all'elettore di dimostrare a terzi la propria scelta. Il problema non è meramente teorico, ma è stato ampiamente discusso nella letteratura crittografica, che ha cercato di sviluppare modelli capaci di garantire la verificabilità senza compromettere la non dimostrabilità del voto[29].

In questa direzione si collocano i lavori di Chaum e Benaloh, che hanno introdotto soluzioni crittografiche volte a evitare che l'elettore disponga di una "ricevuta" utilizzabile per provare la propria scelta. Tali modelli, tuttavia, presentano limiti applicativi significativi, soprattutto quando vengono integrati in sistemi complessi e utilizzati su larga scala[30]. La difficoltà non risiede soltanto nella progettazione matematica dei protocolli, ma nella loro implementazione concreta in contesti reali, caratterizzati da una pluralità di attori, dispositivi e infrastrutture.

L'introduzione della blockchain accentua ulteriormente questa tensione. La registrazione permanente e distribuita delle operazioni, sebbene garantisca elevati livelli di integrità, può generare una quantità di informazioni che, nel tempo, rendono possibile la ricostruzione di relazioni tra elettori e voti, anche attraverso l'analisi di metadati o correlazioni indirette[31]. Come evidenziato dalla letteratura più recente, il problema non è tanto la presenza di un identificatore diretto, quanto la possibilità di combinare dati diversi per ottenere inferenze attendibili sulla scelta elettorale[32].

Su questo punto, anche la dottrina giuridica più recente ha iniziato a interrogarsi in modo critico. In particolare, Caterina e Giannelli sottolineano come il paradigma della verificabilità tecnologica non possa essere assunto automaticamente come equivalente funzionale della fiducia democratica, evidenziando il rischio che l'accento sulla trasparenza finisca per comprimere le garanzie sostanziali del voto, tra cui la segretezza[33] . In termini analoghi, la riflessione interdisciplinare ha posto l'attenzione sulla necessità di considerare il sistema di voto nel suo complesso, evidenziando come l'affidabilità non possa essere garantita esclusivamente attraverso proprietà tecniche della piattaforma[34].

Le principali organizzazioni internazionali hanno mostrato una crescente cautela su questo punto. Le linee guida del National Institute of Standards and Technology e i documenti

CamminoDiritto.it
ISSN 2532-9871

dell'OSCE/ODIHR sottolineano come la sicurezza e la segretezza del voto non possano essere garantite esclusivamente attraverso soluzioni tecnologiche, ma richiedano una valutazione complessiva dell'intero sistema elettorale[35]. In modo analogo, il Consiglio d'Europa ha evidenziato come l'adozione del voto elettronico debba essere accompagnata da rigorose garanzie, soprattutto nei contesti di voto remoto[36].

Ne deriva che il problema non può essere risolto attraverso un semplice perfezionamento tecnico delle soluzioni esistenti. Piuttosto, esso richiede una riflessione più ampia sull'equilibrio tra valori costituzionali: la trasparenza e la verificabilità sono elementi essenziali per la legittimazione del processo elettorale, ma non possono essere perseguite a scapito della segretezza e della libertà del voto.

6. Esperienze comparate e standard internazionali: un approccio prudente al voto elettronico

L'analisi delle esperienze comparate e degli standard internazionali in materia di voto elettronico consente di cogliere con maggiore chiarezza i limiti e le criticità delle soluzioni basate su blockchain. L'orientamento prevalente, sia a livello istituzionale sia nella letteratura tecnico-giuridica, è infatti caratterizzato da un approccio prudente, se non apertamente critico, nei confronti dell'impiego del voto remoto digitale nelle elezioni politiche.

In ambito europeo, la Commissione di Venezia ha da tempo individuato i principi fondamentali delle elezioni democratiche, includendo espressamente la segretezza del voto tra i requisiti imprescindibili. In tale contesto, la segretezza non è considerata una mera formalità, ma una condizione sostanziale che deve essere garantita anche attraverso l'assetto tecnico-organizzativo del sistema elettorale[37]. Successivamente, la stessa Commissione ha ulteriormente precisato come determinate pratiche – quali la pubblicazione di informazioni sulla partecipazione al voto – possano incidere indirettamente sulla segretezza, evidenziando così la rilevanza anche dei dati "periferici" rispetto al contenuto del voto[38].

Un approccio analogo emerge nei documenti del Consiglio d'Europa, che ha elaborato specifiche raccomandazioni sugli standard per il voto elettronico. In particolare, la Raccomandazione CM/Rec(2017)5 sottolinea come l'introduzione di sistemi di e-voting debba essere accompagnata da garanzie rigorose in materia di sicurezza, trasparenza e segretezza, insistendo sulla necessità di mantenere un elevato livello di fiducia pubblica nel processo elettorale[39]. Già nella precedente Raccomandazione Rec(2004)11, il Consiglio d'Europa aveva evidenziato che l'adozione del voto elettronico non può comportare una riduzione delle garanzie rispetto ai sistemi tradizionali, ma deve

CamminoDiritto.it
ISSN 2532-9871

assicurare un livello di tutela almeno equivalente[40].

Anche l'OSCE/ODIHR ha sviluppato linee guida dettagliate per l'osservazione delle nuove tecnologie di voto, evidenziando come i sistemi elettronici introducano nuove superfici di rischio che richiedono un'attenta valutazione. In particolare, viene sottolineato come la complessità tecnica dei sistemi possa ridurre la trasparenza effettiva del processo, rendendo difficile per osservatori e cittadini comprendere e verificare le operazioni elettorali[41]. Tale rilievo appare particolarmente significativo nel contesto della blockchain, dove la trasparenza formale dei dati non coincide necessariamente con la comprensibilità del sistema.

Sul piano extraeuropeo, il rapporto delle National Academies of Sciences statunitensi rappresenta uno dei contributi più autorevoli in materia. Il documento evidenzia in modo chiaro i rischi associati al voto elettronico remoto, raccomandando di evitarne l'uso nelle elezioni politiche a causa delle vulnerabilità strutturali che caratterizzano tali sistemi[42]. In particolare, si sottolinea come la sicurezza del voto non possa essere garantita esclusivamente attraverso soluzioni tecnologiche, ma dipenda da un insieme complesso di fattori, tra cui l'integrità dei dispositivi, la sicurezza delle reti e la gestione delle identità digitali.

In termini analoghi, il National Institute of Standards and Technology ha sviluppato linee guida che pongono l'accento sulla necessità di garantire sistemi di voto verificabili, ma al tempo stesso resilienti rispetto a manipolazioni e attacchi. Il concetto di software independence, elaborato da Rivest e Wack, risulta particolarmente rilevante in questo contesto, in quanto sottolinea che l'affidabilità del risultato elettorale non deve dipendere esclusivamente dal corretto funzionamento del software[43]. Tale principio assume un rilievo ancora maggiore nei sistemi basati su blockchain, nei quali la fiducia tende a essere trasferita dall'istituzione al codice.

Le esperienze comparate mostrano, inoltre, una certa cautela anche nell'adozione concreta del voto elettronico. In diversi ordinamenti, progetti di e-voting sono stati sospesi o ridimensionati a seguito di criticità emerse sul piano della sicurezza e della trasparenza. Il caso svizzero, ad esempio, ha evidenziato come anche sistemi avanzati possano presentare vulnerabilità significative, soprattutto in relazione ai protocolli crittografici e alla loro implementazione[44]. Analogamente, le analisi sul sistema Voatz negli Stati Uniti hanno contribuito a rafforzare un orientamento prudente, evidenziando i rischi connessi al voto remoto su dispositivi personali[45].

Nel complesso, il quadro comparato suggerisce che l'introduzione del voto elettronico – e, a maggior ragione, del voto su blockchain – richiede un approccio graduale e attentamente

CamminoDiritto.it
ISSN 2532-9871

calibrato, che tenga conto non solo delle potenzialità tecnologiche, ma anche delle implicazioni costituzionali e delle condizioni concrete di utilizzo. In particolare, emerge con chiarezza come la segretezza del voto costituisca un parametro particolarmente sensibile, che non può essere sacrificato in nome dell'innovazione tecnologica senza incidere sulla qualità democratica del sistema.

7. Segretezza del voto e limiti della traducibilità tecnica: verso una lettura costituzionalmente orientata

L'analisi svolta consente di evidenziare come il principio di segretezza del voto, nella sua configurazione costituzionale, non sia facilmente traducibile in termini puramente tecnici. La difficoltà non dipende soltanto dai limiti delle soluzioni attualmente disponibili, ma dalla natura stessa della garanzia, che si colloca all'incrocio tra dimensione giuridica, istituzionale e materiale del processo elettorale. In altri termini, la segretezza non appare come una proprietà del sistema, ma come il risultato di un equilibrio complesso tra regole, contesti e condizioni di esercizio del voto[46].

In questa prospettiva, il tentativo di "ingegnerizzare" integralmente la segretezza attraverso protocolli crittografici e architetture distribuite rischia di risultare riduttivo. Come evidenziato nella letteratura tecnico-giuridica, anche i sistemi più avanzati, progettati per garantire anonimato e verificabilità, restano esposti a vulnerabilità che derivano non solo dal codice, ma dall'interazione tra utenti, dispositivi e infrastrutture[47]. Il punto è che la segretezza costituzionale non richiede semplicemente l'assenza di un identificatore diretto, ma l'impossibilità sostanziale di ricostruire la scelta individuale, anche attraverso inferenze indirette.

Tale impostazione trova un importante riscontro anche nella riflessione giuridica più recente. In particolare, Caterina e Giannelli sottolineano come il voto elettronico, specie se basato su tecnologie decentralizzate, imponga una revisione critica dei parametri costituzionali, senza tuttavia poter prescindere da essi. La segretezza, in questa prospettiva, non può essere reinterpretata in funzione delle possibilità tecnologiche, ma deve continuare a operare come limite e parametro di valutazione delle soluzioni adottate [48].

Un ulteriore elemento di criticità riguarda il rapporto tra segretezza e contesto di esercizio del voto. Come già evidenziato, il passaggio dal voto "presidiato" al voto remoto comporta una trasformazione profonda delle condizioni materiali in cui la volontà elettorale si forma ed è espressa. In tale contesto, la tecnologia non è in grado di sostituire integralmente le garanzie ambientali del seggio elettorale, che svolgono una funzione essenziale nel prevenire forme di coercizione o influenza indebita[49]. Ne deriva che la

CamminoDiritto.it
ISSN 2532-9871

segretezza non può essere valutata esclusivamente in relazione alla struttura del sistema, ma deve essere considerata anche alla luce del contesto in cui esso opera.

Sotto questo profilo, appare significativo il richiamo, ricorrente nei documenti internazionali, alla necessità di considerare il processo elettorale nella sua interezza. Le linee guida del NIST e i documenti dell'OSCE/ODIHR insistono sul fatto che la sicurezza e l'affidabilità del voto non possono essere garantite attraverso singole soluzioni tecniche, ma richiedono un approccio sistemico, che tenga conto di tutte le fasi del processo elettorale[50]. Tale impostazione appare pienamente coerente con una lettura costituzionalmente orientata dell'art. 48 Cost., che non si limita a prescrivere requisiti formali, ma impone la realizzazione effettiva delle garanzie del voto.

In questa prospettiva, il problema della compatibilità tra blockchain e segretezza del voto non può essere risolto attraverso un semplice adattamento delle tecnologie esistenti, ma richiede una riflessione più ampia sul rapporto tra diritto e tecnica. La questione non è se la tecnologia possa essere resa compatibile con il principio di segretezza, ma in quale misura tale compatibilità possa essere raggiunta senza alterare il significato costituzionale della garanzia stessa.

Ne consegue che l'introduzione di sistemi di voto basati su blockchain deve essere valutata con particolare cautela, evitando sia approcci entusiastici sia chiusure pregiudiziali. Piuttosto, appare necessario sviluppare strumenti di analisi capaci di cogliere le interazioni tra architetture tecnologiche e principi costituzionali, mantenendo fermo il ruolo della Costituzione come parametro di riferimento ultimo per la valutazione delle innovazioni nel campo elettorale.

8. Conclusioni

L'analisi svolta consente di evidenziare come il rapporto tra blockchain, smart contract e voto elettronico si collochi in una zona di tensione non facilmente risolvibile tra innovazione tecnologica e principi costituzionali. In particolare, il principio di segretezza del voto, così come delineato dall'art. 48 Cost., si rivela difficilmente compatibile con modelli tecnologici fondati su registrazione persistente, verificabilità diffusa e tracciabilità delle operazioni.

Ciò non implica, tuttavia, una conclusione definitiva circa l'incompatibilità in astratto tra blockchain e voto elettronico. Piuttosto, l'analisi suggerisce la necessità di distinguere tra le potenzialità teoriche delle tecnologie e le condizioni concrete della loro implementazione. Le soluzioni tecniche attualmente disponibili, pur offrendo strumenti avanzati di sicurezza e controllo, non sembrano ancora in grado di garantire un livello di

CamminoDiritto.it
ISSN 2532-9871

tutela pienamente conforme alla nozione costituzionale di segretezza, intesa come impossibilità sostanziale di ricostruzione del voto individuale[51].

In questo contesto, appare particolarmente rilevante il rischio di una traslazione impropria del concetto di fiducia: dalla fiducia nelle istituzioni e nelle procedure democratiche a una fiducia nella tecnologia e nei suoi meccanismi di funzionamento. Come evidenziato nella letteratura più recente, tale spostamento non è neutrale, ma comporta una ridefinizione dei presupposti della legittimazione democratica, che non può essere affidata esclusivamente a soluzioni tecniche, per quanto sofisticate[52].

Un ulteriore elemento di cautela deriva dalla considerazione del contesto concreto in cui il voto viene esercitato. Il passaggio da un voto presidiato a forme di voto remoto comporta una trasformazione delle condizioni materiali di espressione della volontà elettorale, con possibili ricadute sulla libertà e sulla segretezza del voto. In tale prospettiva, il problema non riguarda soltanto la sicurezza dell'infrastruttura, ma la capacità del sistema di garantire un ambiente nel quale l'elettore possa esprimersi senza pressioni o condizionamenti[53].

Le esperienze comparate e gli standard internazionali confermano, sotto questo profilo, un orientamento improntato alla prudenza. Le principali organizzazioni internazionali sottolineano come l'introduzione del voto elettronico debba essere accompagnata da garanzie rigorose e da una valutazione complessiva del sistema elettorale, evidenziando i rischi connessi al voto remoto e alla complessità delle infrastrutture digitali[54]. Tale impostazione appare coerente con una lettura dell'art. 48 Cost. che attribuisce alla segretezza una funzione non meramente formale, ma sostanziale, quale presidio della libertà politica.

Alla luce di tali considerazioni, sembra opportuno evitare sia approcci entusiastici, che tendano a sovrastimare le capacità delle tecnologie emergenti, sia posizioni aprioristicamente contrarie all'innovazione. Piuttosto, l'analisi suggerisce la necessità di sviluppare un dialogo continuo tra diritto e tecnica, capace di individuare soluzioni che, pur valorizzando le potenzialità delle nuove tecnologie, non compromettano il nucleo essenziale delle garanzie costituzionali.

In questa prospettiva, il principio di segretezza del voto si configura non solo come un limite, ma anche come un criterio guida per la progettazione e la valutazione dei sistemi di voto elettronico. Esso impone di interrogarsi non soltanto su ciò che è tecnicamente possibile, ma su ciò che è costituzionalmente ammissibile, mantenendo ferma la centralità della persona e della libertà politica nel processo democratico.

CamminoDiritto.it
ISSN 2532-9871

CamminoDiritto.it
ISSN 2532-9871

Note e riferimenti bibliografici

[1]A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, Princeton, Princeton University Press, 2016; ove si evidenzia come l'immutabilità dei registri distribuiti derivi dalla combinazione tra strutture crittografiche e meccanismi di consenso, rendendo estremamente onerosa la modifica retroattiva dei dati.

[2] Art. 48 Cost.; cfr. SENATO DELLA REPUBBLICA, Il diritto di voto e la legge elettorale, in www.senatoragazzi.it, che ricostruisce i caratteri essenziali del suffragio nell'ordinamento costituzionale italiano.

[3] M. ARMANNO, Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014, in Riv. AIC, 2014, 4, il quale sottolinea come le garanzie del voto abbiano natura "strutturale", incidendo direttamente sulla qualità democratica dell'ordinamento.

[4]C.E.D.U., 6 ottobre 2005, Hirst c. Regno Unito (n. 2); C.E.D.U., 15 marzo 2012, Sitaropoulos e Giakoumopoulos c. Grecia, nelle quali la Corte europea dei diritti dell'uomo ribadisce che il diritto di voto deve essere accompagnato da garanzie idonee a preservarne l'effettività e la libertà.

[5] VENICE COMMISSION, Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report, CDL-AD (2002)023rev, punto I.3.2, ove la segretezza è qualificata come requisito imprescindibile delle elezioni democratiche, da assicurare anche sul piano tecnico-operativo.

[6]R. KRIMMER – S. TRIESSNIG – M. VOLKAMER, The Development of Remote E-Voting Around the World: A Review of Roads and Directions, in Proc. 1st Int. Workshop on Electronic Voting (EVOTE), 2004; R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-Voting.CC, 2006, che evidenziano come il voto remoto esponga l'elettore a rischi di coercizione e compromissione dell'anonimato non eliminabili mediante sole soluzioni tecnologiche.

[7] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, Going from Bad to Worse: From Internet Voting to Blockchain Voting, in J. Cybersecur., 2021, 7(1), che dimostra come i sistemi di blockchain voting non risolvano, ma talvolta amplifichino le criticità già note dell'e-voting.

[8] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, Securing the Vote. Protecting American Democracy, Washington D.C., National Academies Press, 2018, che sottolinea l'elevato livello di rischio associato ai sistemi di voto elettronico remoto, raccomandandone un utilizzo estremamente prudente.

[9] Art. 48 Cost.; cfr. anche SENATO DELLA REPUBBLICA, Servizio Studi, Il diritto di voto e la legge elettorale, in www.senatoragazzi.it. La letteratura costituzionalistica recente insiste sul carattere "strutturale" delle garanzie del voto, non riducibili a meri aspetti procedurali: v. M. ARMANNO, Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014, in Riv. AIC, 2014, 4.

[10]Sul punto, in prospettiva tecnico-giuridica, v. D. CHAUM, Secret-Ballot Receipts: True Voter-Verifiable Elections, in IEEE Secur. Privacy, 2004, 2(1); J. BENALOH, Simple Verifiable Elections, in USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), 2006. La rilevanza di queste categorie, pur nate nel lessico informatico, è evidente anche per il giurista, poiché esse esprimono il problema classico della non dimostrabilità del voto.

[11] Sul nesso tra voto remoto e indebolimento della segretezza sostanziale, v. R. KRIMMER – S. TRIESSNIG – M. VOLKAMER, The Development of Remote E-Voting Around the World: A Review of Roads and Directions, in Proc. 1st Int. Workshop on Electronic Voting (EVOTE), 2004; sui rischi di condizionamento ambientale connessi alle forme di voto non presidiato e remoto, si veda, invece, G. VASINO, La tutela della segretezza del voto: profili ricostruttivi e problematiche attuali, in Nomos. Le attualità nel diritto, 2020, 1, disponibile anche in Nomos – Le attualità nel diritto, che ricostruisce in chiave sistematica il principio di segretezza e ne evidenzia le criticità attuali.

[12] In questa prospettiva, appare utile il confronto con il voto per corrispondenza, che mostra come il problema della segretezza non riguardi solo la possibilità di ricostruzione tecnica del voto, ma anche la perdita del presidio

ambientale proprio del seggio. In termini più generali, v. R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-Voting.CC, 2006.

[13] VENICE COMMISSION, Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report, CDL-AD (2002)023rev, punto I.3.2; v. anche VENICE COMMISSION, Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections, CDL-AD (2010)037.

[14] E. CATERINA – M. GIANNELLI, Il voto ai tempi del Blockchain: per una rinnovata valutazione costituzionale del voto elettronico, in Riv. AIC, 2021, 4. Il contributo affronta espressamente il rapporto tra parametri costituzionali del voto e impiego della blockchain, con attenzione ai profili di libertà, segretezza e sostenibilità costituzionale del voto remoto.

[15] C. CHIARIELLO, Voto elettronico e principio di segretezza tra regola ed eccezioni, in Consulta Online, Studi, 2019, disponibile in www.giurcost.org, che analizza criticamente il voto elettronico, in particolare nella forma del c.d. home vote, in rapporto alle garanzie di libertà e segretezza.

[16] A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, cit., ove si descrive il funzionamento dei registri distribuiti e il ruolo della crittografia nel garantire l'immutabilità dei dati.

[17] Sul ruolo dei metadati e delle possibili correlazioni indirette, v. S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., che evidenziano come l'anonimato nei sistemi di voto digitale sia estremamente difficile da garantire in presenza di architetture complesse e distribuite.

[18] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., i quali sottolineano come la blockchain non elimini le vulnerabilità dei sistemi di voto remoto, ma si limiti ad aggiungere un ulteriore livello di complessità.

[19]NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, Securing the Vote. Protecting American Democracy, cit., che raccomanda espressamente di evitare l'uso del voto via Internet per elezioni politiche, a causa dei rischi elevati per sicurezza e integrità.

[20] D. CHAUM, Secret-Ballot Receipts: True Voter-Verifiable Elections, in IEEE Secur. Privacy, 2004, 2(1).; J. BENALOH, Simple Verifiable Elections, in USENIX/ACCURATE EVT Workshop, 2006. Tali lavori introducono modelli crittografici che cercano di conciliare verificabilità e segretezza, evitando che l'elettore possa dimostrare la propria scelta.

[21]In termini più generali, sul rapporto tra sicurezza, trasparenza e limiti delle soluzioni tecnologiche, v. B. SCHNEIER, Beyond Fear. Thinking Sensibly About Security in an Uncertain World, New York, 2003, che evidenzia come ogni sistema di sicurezza comporti trade-off inevitabili tra esigenze concorrenti.

[22] M. SPECTER – J. KOPPEL – D. WEITZNER, The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, in Proc. 29th USENIX Security Symp., 2020. Lo studio, basato anche su tecniche di reverse engineering dell'applicazione, evidenzia vulnerabilità sia lato client sia lato server, mettendo in discussione la sicurezza complessiva del sistema.

[23] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., ove si sottolinea come la blockchain non intervenga sulle criticità relative ai dispositivi dell'elettore e alla trasmissione del voto.

[24] In questo senso, la compromissione dell'infrastruttura può incidere indirettamente anche sulla segretezza, consentendo la raccolta di informazioni sensibili o la ricostruzione di pattern di voto; sul punto, v. ancora M. SPECTER – J. KOPPEL – D. WEITZNER, op. cit.

[25] Sul tema del voto remoto e dei rischi di coercizione, v. R. KRIMMER – M. VOLKAMER, Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, Working Paper Series on Electronic Voting and Participation, E-Voting.CC, 2006, n. 01.

[26] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Voluntary Voting System Guidelines (VVSG), Gaithersburg, 2021; OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, Varsavia, 2013; COUNCIL OF EUROPE, Recommendation CM/Rec (2017)5 on standards for

e-voting, 2017. Tali documenti evidenziano come la sicurezza dei sistemi di voto debba essere valutata in modo sistemico e non limitato a singole componenti tecnologiche.

[27] A. NARAYANAN – J. BONNEAU – E. FELTEN – A. MILLER – S. GOLDFEDER, Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, cit. Il volume, pur non riferito specificamente al voto elettronico, è rilevante per comprendere le proprietà strutturali della blockchain (immutabilità, trasparenza, distribuzione), che costituiscono il presupposto tecnico delle applicazioni elettorali e ne spiegano le potenziali tensioni con la segretezza del voto.

[28] VENICE COMMISSION, Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report, CDL-AD (2002)023rev, punto I.3.2.

[29] J. BENALOH, op. cit. L'Autore introduce modelli di voto verificabile che consentono il controllo del processo senza compromettere la segretezza individuale, ponendo le basi teoriche dei sistemi end-to-end verifiable.

[30] D. CHAUM, op. cit., ove il contributo sviluppa il concetto di receipt-freeness, ossia l'impossibilità per l'elettore di dimostrare a terzi la propria scelta. Si tratta di un requisito essenziale per prevenire fenomeni di coercizione o compravendita del voto, ma la sua implementazione concreta nei sistemi digitali presenta difficoltà significative.

[31]S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit.

[32] Ibid. In particolare, viene sottolineato che l'anonimato nei sistemi digitali non può essere valutato solo in termini di assenza di identificatori diretti, ma deve tener conto della possibilità di inferenze ottenute attraverso l'analisi combinata di metadati e comportamenti di rete.

[33] E. CATERINA – M. GIANNELLI, op. cit., ove gli autori mettono in guardia contro l'equivalenza tra trasparenza tecnologica e affidabilità democratica, sottolineando come l'accento sulla verificabilità possa entrare in tensione con le garanzie costituzionali del voto, in particolare la segretezza.

[34] R. RIVEST – J. WACK, On the Notion of "Software Independence" in Voting Systems, Gaithersburg, 2006. Il concetto di software independence evidenzia che un sistema elettorale non può dirsi sicuro se l'integrità del risultato dipende esclusivamente dal corretto funzionamento del software, richiamando la necessità di meccanismi di verifica indipendenti.

[35] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Voluntary Voting System Guidelines (VVSG), Gaithersburg, 2021; OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, Varsavia, 2013.

[36] COUNCIL OF EUROPE, Recommendation CM/Rec (2017)5 on standards for e-voting, 2017.

[37] VENICE COMMISSION, Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report, CDL-AD (2002)023 rev, punto I.3.2.

[38] VENICE COMMISSION, Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections, CDL-AD (2010)037.

[39] COUNCIL OF EUROPE, Recommendation CM/Rec (2017)5 on standards for e-voting, 2017.

[40] COUNCIL OF EUROPE, Recommendation Rec (2004)11 on legal, operational and technical standards for e-voting, 2004. La Raccomandazione stabilisce che il voto elettronico deve rispettare i medesimi principi del voto tradizionale.

[41] OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, Warsaw, 2013.

[42] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, Securing the Vote: Protecting American Democracy, Washington D.C., 2018.

[43] R. RIVEST – J. WACK, op. cit. Il concetto di «software independence» rappresenta uno dei passaggi teorici più rilevanti nella riflessione sui sistemi di voto elettronico: un sistema elettorale può dirsi affidabile solo se eventuali errori o compromissioni del software non sono in grado di alterare il risultato senza essere rilevati. In questa prospettiva, la fiducia non può essere interamente delegata al codice, ma deve poggiare su meccanismi di verifica indipendenti. Tale impostazione risulta particolarmente problematica nei sistemi basati su blockchain, nei quali la

CamminoDiritto.it
ISSN 2532-9871

correttezza del processo è spesso ricondotta alla sola integrità dell'infrastruttura tecnica.

[44] A. ESSEX, Analysis of the Swiss Post E-Voting System Audit Scope 1: Cryptographic Protocol, report alla Cancelleria Federale Svizzera, 26 novembre 2021. Il report costituisce uno dei principali esempi di audit crittografico applicato a sistemi reali di voto elettronico. L'analisi del sistema Swiss Post ha evidenziato criticità significative nella progettazione del protocollo, dimostrando come anche soluzioni sviluppate con elevati standard tecnici possano presentare vulnerabilità rilevanti. Il caso conferma che la sicurezza dei sistemi elettorali digitali non può essere presunta sulla base della complessità tecnologica, ma richiede verifiche indipendenti e continue.

[45] M. SPECTER, J. KOPPEL, D. WEITZNER, op. cit. Lo studio, utilizzato in alcune sperimentazioni negli Stati Uniti, evidenzia vulnerabilità che riguardano l'intero ciclo del voto: dal dispositivo dell'elettore alla trasmissione dei dati fino all'infrastruttura server. Particolarmente rilevante è la conclusione secondo cui i problemi di sicurezza emergono già a monte dell'eventuale utilizzo della blockchain, mettendo in luce come l'introduzione di registri distribuiti non sia di per sé idonea a risolvere le criticità strutturali del voto remoto.

[46] Art. 48 Cost.; cfr. M. ARMANNO, op. cit. Tali requisiti non possono essere considerati isolatamente, ma operano in modo integrato, incidendo direttamente sulla legittimazione del processo democratico. In questa prospettiva, la segretezza non si esaurisce nell'anonimato tecnico, ma richiede l'assenza di qualsiasi possibilità di ricostruzione, anche indiretta, della scelta elettorale.

[47] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit., ove si mette in luce come il passaggio da sistemi di voto via internet a soluzioni basate su blockchain non risolva i problemi strutturali già noti, ma possa anzi accentuarli. In particolare, viene evidenziato come l'adozione di registri distribuiti non elimini i rischi connessi all'identificazione indiretta degli elettori, soprattutto in presenza di dati persistenti e pubblicamente accessibili.

[48] E. CATERINA – M. GIANNELLI, op. cit. Gli Autori sottolineano la necessità di evitare una sovrapposizione tra affidabilità tecnica e legittimazione costituzionale del voto. In particolare, viene evidenziato come la trasparenza algoritmica non possa essere considerata, di per sé, equivalente alla fiducia democratica, richiedendo invece una verifica alla luce dei principi costituzionali, tra cui la segretezza del voto.

[49] R. KRIMMER, M. VOLKAMER, op. cit., con specifico riferimento all'analisi sui rischi per l'anonimato nei sistemi di voto elettronico, con particolare attenzione alle modalità di voto remoto. Gli Autori evidenziano come la perdita di controllo sull'ambiente di voto possa incidere non solo sulla riservatezza tecnica, ma anche sulla libertà sostanziale dell'elettore, esponendolo a possibili pressioni esterne.

[50] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Voluntary Voting System Guidelines (VVSG), 2021; OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, 2013.

[51] S. PARK – M. SPECTER – N. NARULA – R. L. RIVEST, op. cit.; NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, Securing the Vote: Protecting American Democracy, Washington D.C., 2018. I due contributi, pur diversi per approccio, convergono nel mettere in discussione l'affidabilità dei sistemi di voto remoto basati su tecnologie digitali. In particolare, Park et al. evidenziano come la blockchain non risolva le criticità strutturali dell'internet voting, mentre il rapporto delle National Academies assume una posizione più netta, sottolineando come, allo stato attuale, non esistano condizioni tecniche sufficienti per garantire sicurezza e segretezza nel voto via internet. Nel loro insieme, tali lavori suggeriscono che il problema non è meramente tecnologico, ma investe l'architettura complessiva del processo elettorale.

[52] E. CATERINA – M. GIANNELLI, op. cit. Con specifico riferimento alla parte in cui si sottolinea che il rischio di una progressiva sostituzione della fiducia istituzionale con una fiducia tecnologica, evidenziando come la legittimazione del processo elettorale non possa essere delegata alla sola correttezza del sistema tecnico. In questa prospettiva, la blockchain non rappresenta una soluzione neutra, ma introduce un diverso modello di fiducia che deve essere valutato criticamente alla luce dei principi costituzionali, in particolare della segretezza e della libertà del voto.

[53] R. KRIMMER – M. VOLKAMER, op. cit. Il lavoro evidenzia come le minacce all'anonimato nei sistemi di voto elettronico non derivino esclusivamente da vulnerabilità tecniche, ma anche dal contesto operativo in cui il voto è espresso. In particolare, gli Autori mostrano come il voto remoto, non presidiato, possa compromettere non solo la riservatezza del voto, ma anche la libertà dell'elettore, esponendolo a possibili pressioni o condizionamenti difficilmente rilevabili.

[54] VENICE COMMISSION, Code of Good Practice in Electoral Matters, 2002; COUNCIL OF EUROPE,

CamminoDiritto.it
ISSN 2532-9871

Recommendation CM/Rec (2017)5, 2017; OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, 2013

BIBLIOGRAFIA

ARMANNO M., Diritto di voto, rappresentanza ed eguaglianza del suffragio dopo la sentenza n. 1 del 2014, in Rivista AIC, 2014, 4.

BENALOH J., Simple Verifiable Elections, in USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), 2006.

CATERINA E., GIANNELLI M., Il voto ai tempi del Blockchain: per una rinnovata valutazione costituzionale del voto elettronico, in Rivista AIC, 2021, 4.

CHAUM D., Secret Ballot Receipts: True Voter Verifiable Elections, in IEEE Security & Privacy, 2004, 2(1).

CHIARIELLO C., Voto elettronico e principio di segretezza tra regola ed eccezioni, in Consulta Online, Studi, 2019.

CONSIGLIO D'EUROPA, Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting, 2004.

CONSIGLIO D'EUROPA, Recommendation CM/Rec(2017)5 on standards for e-voting, 2017.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, Hirst c. Regno Unito (n. 2), 6 ottobre 2005.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, Sitaropoulos e Giakoumopoulos c. Grecia, 15 marzo 2012.

COSTITUZIONE DELLA REPUBBLICA ITALIANA, art. 48.

ESSEX A., Analysis of the Swiss Post E-Voting System Audit Scope 1: Cryptographic Protocol, report alla Cancelleria Federale Svizzera, 26 novembre 2021.

KRIMMER R., TRIESSNIG S., VOLKAMER M., The Development of Remote E-Voting Around the World: A Review of Roads and Directions, in Proceedings of the 1st International Workshop on Electronic Voting (EVOTE), 2004.

KRIMMER R., VOLKAMER M., Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting, in Working Paper Series on Electronic Voting and Participation, E-Voting.CC, 2006.

NARAYANAN A., BONNEAU J., FELTEN E., MILLER A., GOLDFEDER S., Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, Princeton, Princeton University Press, 2016.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, Securing the Vote: Protecting American Democracy, Washington D.C., National Academies Press, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), Voluntary Voting System Guidelines (VVSG), Gaithersburg, 2021.

OSCE/ODIHR, Handbook for the Observation of New Voting Technologies, Warsaw, 2013.

PARK S., SPECTER M., NARULA N., RIVEST R. L., Going from Bad to Worse: From Internet Voting to Blockchain Voting, in Journal of Cybersecurity, 2021, 7(1).

RIVEST R. L., WACK J., On the Notion of "Software Independence" in Voting Systems, Gaithersburg, 2006.

SCHNEIER B., Beyond Fear: Thinking Sensibly About Security in an Uncertain World, New York, Copernicus Books, 2003.

SENATO DELLA REPUBBLICA, Il diritto di voto e la legge elettorale, disponibile su www.senatoragazzi.it.

SPECTER M., KOPPEL J., WEITZNER D., The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, in Proceedings of the 29th USENIX Security Symposium, 2020.

CamminoDiritto.it
ISSN 2532-9871

VENICE COMMISSION, Code of Good Practice in Electoral Matters. Guidelines and Explanatory Report, CDL-AD (2002)023rev.

VENICE COMMISSION, Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections, CDL-AD (2010)037.

---

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina:
https://rivista.camminodiritto.it/articolo.asp?id=11547