UNIVERSITÁ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in Giurisprudenza

a.a. 2023/2024

LA TECNOLOGIA BLOCKCHAIN APPLICATA AL VOTO ELETTRONICO: OPPORTUNITÁ E NUOVE SFIDE.

Relatore: Chiar.mo Prof. CLAUDIO SARRA

Controrelatore: Chiar.mo Prof. SARZO MATTEO

Laureanda: Corvi Tytynyuk Olga Igorivna

Matricola 1167822

Indice

Introduzione

La tecnologia blockchain è una delle innovazioni più rilevanti nel settore digitale le cui caratteristiche hanno consentito la sua applicazione in diversi settori. Il presente lavoro si pone come obiettivo di studiare e analizzare l'applicazione della tecnologia blockchain nel voto elettronico mettendone in luce i pregi, ma anche i difetti.

Il primo capitolo offre una panoramica sulla tecnologia blockchain partendo dalle sue origini e proseguendo nell'analisi delle singole componenti con particolare riguardo agli algoritmi di consenso e alle tipologie di blockchain conosciute. Vengono, poi, esposti alcuni casi di utilizzo prendendo come esempio le cc.dd. città intelligenti e la sanità digitale. Il capitolo si conclude con una breve riflessione sul legame intercorrente tra datificazione e blockchain.

Il secondo capitolo analizza il concetto di democrazia sin dalle origini ai giorni nostri con particolare attenzione agli elementi della partecipazione elettorale e della tutela dei diritti fondamentali.

Il terzo capitolo studia la nozione di *e-democracy* come ulteriore sfumatura del concetto di democrazia scaturita dalla perdurante crisi della democrazia rappresentativa e dei partiti politici, nonché dall'ingerenza sempre maggiore delle ICT e dei nuovi mezzi di comunicazione in politica evidenziati nei fenomeni delle bolle di filtro e delle camere di eco. Si prosegue, poi, con l'analisi di alcune esperienze di democrazia elettronica ponendo uno sguardo all'Estonia e al funzionamento del *remote Internet voting* e all'Italia con riferimento al Movimento 5 Stelle e l'utilizzo da parte di esso della piattaforma Rousseau.

Il quarto ed ultimo capitolo affronta la questione del voto elettronico e della applicazione della blockchain in tale settore. Dapprima viene fornita una definizione per quanto più completa possibile di voto elettronico ponendo l'attenzione sullo sviluppo tecnologico a partire dal sistema delle schede perforate al voto online e sulla modalità, ossia presidiata e non presidiata. Successivamente viene analizzata la compatibilità tra la tecnologia blockchain e i principi espressi in materia elettorale soprattutto con riguardo all'articolo 48 della Costituzione. La trattazione prosegue con lo studio delle opportunità che tale tecnologia offre se applicata nel settore elettorale in riferimento alla velocità nello spoglio e alle caratteristiche della trasparenza, sicurezza ed immutabilità. Infine, viene aperta una riflessione sulle difficoltà di applicazione della blockchain al voto elettronico analizzando i problemi della mancanza di standard comuni e della scalabilità.

CAPITOLO I: LA TECNOLOGIA BLOCKCHAIN.

1. La storia delle blockchain

Prima di affrontare questioni di carattere giuridico è necessario descrivere il funzionamento e l'utilizzo di una delle innovazioni tecnologiche più rilevanti nell'ultimo decennio. Il presente paragrafo indagherà le origini avvolte nel mistero della blockchain con accenni di carattere storico e l'analisi del paper di Satoshi Nakamoto, padre del Bitcoin.

1.1. Origine della blockchain

Quando si parla di blockchain la prima cosa che viene in mente è il Bitcoin, prima criptovaluta ad essere creata e messa in funzione. Il Bitcoin è stato teorizzato nel white – paper di Satoshi Nakamoto intitolato "*Bitcoin: a Peer to Peer Electronic Cash System*" del 2008. In realtà, questo libro bianco è frutto di una serie di contributi e ricerche che affondano le proprie radici negli anni '70 del secolo scorso e più precisamente nel 1976[1], anno in cui vi è stata la pubblicazione del primo lavoro accademico in materia intitolato "*New Directions in Cryptography"* di Whitfield Diffie e Martin E. Hellman. Successivamente, a partire dagli anni '80 con l'inizio della diffusione dei computer venne sollevata qualche perplessità circa la protezione dei dati e la privacy. In questo contesto si sviluppò il cc.dd. movimento Cypherpunk, ossia un gruppo di attivisti che "*utilizzano la crittografia informatica per poter favorire cambiamenti politici e sociali"*[2]. Sull'onda di questo movimento, nel 1992 Tim May scrive "*The Crypto Anarchist Manifesto"* ed emerge come la crittografia sia lo strumento più adatto per garantire la protezione della privacy e l'anonimato tra soggetti che intendono comunicare ed interagire tra loro. L'autore è anche consapevole di come la crittografia possa essere utilizzata per fini benevoli, ma anche per commettere reati. Nonostante questa consapevolezza, nel manifesto afferma come *"this will not halt the spread of crypto anarchy"*[3] ossia questo aspetto non fermerà la diffusione della criptoanarchia. Nel 1993, sempre sull'onda del movimento in questione, Eric Hughes firma *"A cypherpunk's Manifesto"* il cui contenuto è più politico e meno tecnico rispetto al testo di Tim May. L'autore si concentra sulla privacy facendo una distinzione tra privacy e segretezza. La prima consiste nel fatto che di una determinata questione solo alcuni ne siano a conoscenza, mentre altri ne sono all'oscuro; la seconda consiste nel fatto che di quella questione nessuno deve sapere qualcosa[4]. La differenza è molto sottile, ma i due concetti differiscono, in quanto la privacy permette alla persona

[1] Emre, 2022
[2] https://www.hola-cripto.com/glossario-criptovalute/cypherpunk-significato/
[3] May, 1992
[4] Hughes, 1993

interessata di selezionare gli argomenti o, meglio, alcuni aspetti della propria esistenza e condividerli con il mondo intero. Il manifesto si conclude con la missione dei Cypherpunk, ossia quella di creare codici informatici per poter garantire privacy e anonimato. Negli anni '90 del secolo scorso inizia la Internet Revolution. In questo contesto di ottimismo e fiducia nei confronti delle nuove tecnologie si inserisce l'articolo di Stuart Haber e W. Scott Stornetta pubblicato nel 1991 intitolato "*How To Time-Stamp a Digital Document"* precursore di uno degli elementi chiave della blockchain, ossia il marcatore temporale. L'obiettivo è quello di poter certificare la data di creazione del documento o la data della sua ultima modifica. Questo è un problema di particolare importanza soprattutto in materia di proprietà intellettuale, infatti la data è un elemento cruciale per poter stabilire la precedenza di un progetto rispetto ad un altro per ottenere il brevetto[5]. Gli autori propongono diverse soluzioni di autenticazione che riguardano i documenti analogici come la annotazione del documento in appositi registri. Se per i documenti analogici il problema della autenticazione non si pone, per i documenti digitali, invece, è presente in quanto sono file che possono essere facilmente alterati. La soluzione proposta è quella di creare un documento sotto algoritmo di hashing che produce un identificativo univoco. Se viene modificato anche un solo bit[6] del file elettronico questo viene sottoposto ad un nuovo hashing e il documento risultante è diverso. È lo stesso funzionamento delle blockchain, le quali utilizzano l'algoritmo SHA-256 per generare le stringhe di hash utilizzate per la crittografia dei blocchi. Ad esempio, in SHA-256 "Ciao" sarebbe *25c73520e69bf229811e8e46ffe7d80471544b9bee15ed25044b86be4115ad*; mentre "Ciao!" risulta *6199ce5b522dbbbcf1f5927eeab860165ad131e1cb6b76aead9c0088a9ef85dd3*[7]. Un altro tassello che si aggiunge al puzzle delle blockchain riguarda la teorizzazione di B-money[8] da parte di Wei Dai. B-money è l'anticipatore, assieme a Bit Gold concettualizzato nel 2005 da Nick Szabo, del Bitcoin ed è un sistema che si basa sull'algoritmo di consenso Proof – of – Work. L'autore descrive due protocolli di funzionamento di cui il primo, piuttosto complesso, risulta essere impraticabile in quanto per poter funzionare necessita l'utilizzo di canali sincronizzati. Il primo protocollo prevede un sistema di database in cui ogni partecipante indica quanti soldi appartengono a ciascun pseudonimo[9]. Il primo passaggio consiste nella creazione di denaro tramite la diffusione di un problema computazionale rimasto irrisolto. L'autore pone due condizioni affinché si crei denaro, ossia (i) deve essere facile valutare l'entità dello sforzo utilizzato per risolvere il problema e (ii) la soluzione non deve avere alcun

[5] Haber & Stornetta, 1991
[6] Il bit, conosciuto anche come binary digit, è una cifra binaria formata da 0 e 1 che, nel linguaggio informatico, rappresenta uno stato come vero/falso, oppure aperto/chiuso. Tratto da: https://www.geopop.it/bit-byte-megabyte-e-gigabyte-cosa-sono-e-che-differenza-ce-tra-queste-unita-di-misura-informatiche/
[7] https://sha256algorithm.com/
[8] Dai, 1998
[9] *Ibidem*

valore pratico né intellettuale[10]. Una volta creato denaro, vi è il trasferimento tra i vari partecipanti che avviene tramite l'esecuzione di contratti il cui contenuto prevede la somma massima che ogni contraente è disposto a prestare in caso di inadempimento, nonché l'accettazione di risolvere eventuali controversie con l'arbitrato. Nel caso in cui non sia presente alcuna disputa, ogni parte diffonde un messaggio che può essere, ad esempio, "*Il contratto si è concluso senza la necessità di prestare riparazioni"* oppure "*Il contratto si conclude con la prestazione delle seguenti riparazioni"*. Successivamente, alla diffusione di tutte le firme, ogni partecipante aggiornerà il proprio database versando la riparazione dovuta all'account di ciascuna parte, eliminerà l'account del contratto e apporterà crediti o addebiti ad esso se lo schema della riparazione lo consente. L'autore, poi, considera l'eventualità per cui non sia possibile concludere un contratto nemmeno con l'arbitrato. In questo caso ciascuna parte diffonderà uno schema di riparazioni allegando argomenti a proprio favore e ogni partecipante prenderà una decisione a riguardo andando a modificare il contratto di conseguenza. È un sistema piuttosto artificioso che richiede l'utilizzo di macchinari con enormi potenzialità di calcolo per la risoluzione dei problemi matematici che permettono la creazione di denaro, macchinari che non tutti possiedono. Il secondo protocollo, invece, prevede una serie di server collegati tra di loro da un canale sincronizzato e i partecipanti di ogni transazione devono verificare che il messaggio sia stato ricevuto con successo e processato correttamente da un numero di server selezionati a random. Dalla sommaria descrizione del funzionamento dei protocolli di B-money si comprende come sia latente l'idea e il funzionamento delle blockchain.

1.2. Il paper di Satoshi Nakamoto

Il 31 ottobre 2008 per molti è una data priva di significato, ma nel mondo della tecnologia segna un evento sparti acque, ossia la pubblicazione del white – paper di Satoshi Nakamoto "*Bitcoin: a Peer to Peer Electronic Cash System".* È un'opera che in sole 9 pagine è riuscita a dar vita a una rivoluzione in campo digitale teorizzando il funzionamento della prima moneta elettronica senza mai nominare la tecnologia alla base, cioè la blockchain, ma spiegandone il funzionamento. Nakamoto, tuttavia, non è il vero nome dell'autore o degli autori, infatti è uno pseudonimo. Nella comunità digitale vi sono stati vani tentativi di individuare chi sia il padre del Bitcoin ed è emersa nel corso degli anni una rosa di nomi, tra cui Nick Szabo, Hal Finney, Dorian Nakamoto, la cui omonimia si rivelerà solo una strana coincidenza e Craig Steven Wright, imprenditore australiano che da anni dichiara di essere l'autore del white - paper, ma le evidenze da lui fornite e i fatti dimostrano il contrario. Le figure, però, su cui gli speculatori si sono concentrati maggiormente sono Szabo e Finney entrambi parte del movimento

[10] *Ibidem*

Cypherpunk. Nick Szabo nel 1994 introdusse la nozione di smart contract e l'attenzione si concentrò su di lui in quanto lo stile di scrittura, facendo un confronto tra le sue pubblicazioni e il white paper, sono molto simili. Inoltre nel 2005 egli aveva teorizzato Bit Gold antenato del Bitcoin. L'attenzione era puntata anche su Hal Finney, prematuramente scomparso nel 2014, in quanto una serie di coincidenze, tra cui il fatto di aver lavorato a lungo sul Bitcoin e l'essere stato il primo al mondo a ricevere una transazione in moneta virtuale, hanno fondato il sospetto che potesse essere Nakamoto. Al di là delle varie congetture su chi vi sia dietro la figura di Nakamoto ciò che è interessante è il testo da lui pubblicato. Nell'introduzione vengono spiegate le ragioni che hanno portato alla teorizzazione della prima criptovaluta e la sua attuazione nel 2009, ossia tutte le transazioni finanziarie avvengono in presenza di un soggetto terzo, quale, ad esempio, la banca o un'autorità pubblica. L'autore sottolinea come l'elemento del trust, ovvero della fiducia, sia una debolezza del sistema, in quanto non si può negare che vi possano essere delle controversie e che le transazioni stesse non sono reversibili. Nakamoto evidenzia, poi, come i tradizionali sistemi di pagamento siano soggetti a frodi. Si può affermare come la pubblicazione del white – paper sia anche una sorta di reazione alla crisi finanziaria del 2008 iniziata con la dichiarazione di fallimento della Lehman Brothers il 15 settembre dello stesso anno. Con la teorizzazione del Bitcoin l'obiettivo che si voleva raggiungere, e che si è raggiunto, era l'ideazione di un sistema alternativo di pagamento, sicuro e privo di soggetti terzi risolvendo, così, il problema della fiducia nella parte terza. Con tale sistema di pagamento alternativo i venditori, da un lato, vengono tutelati contro le frodi e gli acquirenti, dall'altro, vengono protetti con l'implementazione di sistemi di garanzie. L'articolo prosegue con la descrizione del funzionamento del Bitcoin. Essenzialmente, la moneta elettronica viene definita come una catena di firme digitali. Ciascun proprietario trasferisce la moneta al successivo firmando digitalmente un hash della trascrizione precedente e la chiave pubblica del proprietario successivo aggiungendo questi elementi alla "fine" della moneta. Per evitare il problema del double spending, ossia, la situazione per la quale la moneta viene spesa due volte, si utilizza un server di marcatura temporale, vale a dire il *timestamp,* il quale dà prova della data e dell'ora in cui è avvenuta la transazione. Ogni timestamping include la marcatura temporale precedente in hash creando una catena che si aggiunge a quella precedente. In questa maniera viene a crearsi una catena di blocchi, vale a dire la blockchain.

2. Come funzionano le blockchain

A seguito della breve introduzione di carattere storico circa le origini della blockchain e la misteriosa figura di Nakamoto è necessario offrire una panoramica, per quanto accurata possibile, sulle componenti di questa tecnologia innovativa fornendo, in primis, una definizione più accurata di blockchain.

2.1. Che cos'è una blockchain

Nate nel 2008, ma teorizzate ben prima, le blockchain sono conosciute prevalentemente per la loro utilizzazione nel campo delle criptovalute. In letteratura sono presenti una varietà di definizioni, le quali descrivono la blockchain come una catena di blocchi nella quale i dati sono inseriti all'interno di ciascun blocco per mezzo della crittografia di hash e validazione temporale. Ogni blocco è concatenato a quello precedente tramite il richiamo all'hash precedente nel blocco successivo. Da questo legame deriva una delle caratteristiche principali della blockchain, vale a dire l'immutabilità, per cui, una volta che la transazione è stata effettuata, i dati all'interno del blocco non possono più essere modificati. Nel momento in cui vengono effettuate nuove transazioni, ogni nodo le inserisce all'interno di un nuovo blocco che per poter essere aggiunto alla catena deve essere approvato da tutti gli altri nodi della rete. L'approvazione da parte dei nodi avviene tramite un processo di validazione che viene effettuato dai c.d. *miners*, ossia da alcuni nodi specificamente adibiti a tale funzione che, a seconda dell'algoritmo di consenso utilizzato, procedono all'approvazione del nuovo blocco e nel momento in cui la maggior parte dei nodi accetta la transazione, il blocco viene creato e aggiunto alla catena[11]. La blockchain, dunque, si basa su una struttura decentralizzata caratterizzata dalla presenza di più nodi che formano una rete di infinite dimensioni affinché venga garantita la sicurezza e la resilienza della catena. A tal scopo, infatti, ogni partecipante della rete possiede una copia di tutte le operazioni che sono state effettuate. Con tale sistema, dunque, in presenza di nodi disonesti o di un attacco informatico, gli altri nodi della rete detengono una copia delle transazioni effettuate e la blockchain può continuare a funzionare. Nel corso del tempo si sono sviluppate diverse generazioni di blockchain[12], in particolare esse possono essere suddivise in tre corrispondenti ai diversi periodi di evoluzione di tale tecnologia. Partendo dalle origini fino al 2013 vi è la blockchain teorizzata da Nakamoto, ossia il Bitcoin. È una blockchain caratterizzata dall'uso dell'algoritmo Proof – of – Work che garantisce sicurezza e stabilità,

[11] Nakamoto, 2008
[12] Bruschi, Rusconi, & Zoia, 2022

ma anche scarsa produttività, dando vita al problema della scalabilità, oltre alla scarsa sostenibilità dal punto di vista ambientale causato da elevati consumi energetici. Successivamente nel 2013 nasce Ethereum, una nuova tipologia di blockchain il cui funzionamento poggia sugli *smart contract*. Ethereum nasce dalle considerazioni circa i limiti del Bitcoin, il quale consente di eseguire operazioni elementari quali ricevere e inviare denaro, senza la possibilità di apporre delle condizioni, quale ad esempio *"invio X Bitcoin a Tizio, a condizione che la merce che ho ordinato arrivi intatta".* In origine Ethereum utilizzava l'algoritmo del Bitcoin per poi adottare il protocollo di consenso Proof – of – Stake, più efficiente e sostenibile. Infine, vi una nuova era delle blockchain, ossia le c.d. *green blockchain,* le quali promettono di essere più sostenibili e di risolvere alcune problematiche quali la scalabilità[13] e l'interoperabilità[14]. Per quanto riguarda, poi, la sostenibilità, le *green blockchain* abbandonerebbero l'utilizzazione dell'algoritmo Proof – of – Work in favore del Proof – of – Stake eliminando l'utilizzazione di macchinari che necessariamente devono essere dotati di enormi potenzialità di calcolo per risolvere i problemi computazionali forniti dall'algoritmo. Le blockchain di ultima generazione preferiscono l'utilizzazione del Proof – of – Stake in quanto, affinché un nuovo blocco venga creato, non vi è la necessità di risolvere complessi problemi matematici. Nel Proof – of – Stake, infatti, ogni nodo mette a disposizione un certo ammontare di criptovaluta, vale a dire lo *stake*, per poter poi essere selezionato, per lo più in maniera del tutto casuale, per la creazione del nuovo blocco. In questo algoritmo di consenso, quindi, non viene richiesto un elevato consumo di energia elettrica per la creazione dei nuovi blocchi, il che lo rende maggiormente appetibile per le blockchain di nuova generazione particolarmente attente alla questione della sostenibilità energetica. Volgendo, poi, uno sguardo all'aspetto giuridico vi è qualche riferimento a livello sovranazionale circa le blockchain e le Distributed Ledger Technologies. Vi è, infatti, la Risoluzione del Parlamento Europeo del 3 ottobre 2018 la quale evidenzia le opportunità e migliorie che tali tecnologie possono apportare se sfruttate al meglio, tra cui un maggior grado di autonomia dei cittadini fornendo loro la possibilità di controllare i propri dati e decidere quali condividere nel registro. Si evidenzia come queste tecnologie permettano un miglioramento dell'efficienza delle transazioni, dal punto di vista economico, eliminando intermediari e costi di intermediazione. Grazie alle DLT e alle blockchain, inoltre, aumenterebbe il grado di trasparenza e quindi vi sarebbe una conseguente diminuzione della corruzione e dell'evasione fiscale. Il Parlamento Europeo, però, è consapevole del fatto che vi è un certo scetticismo nell'utilizzazione di questi sistemi a registro distribuito, pertanto invita gli Stati membri e le stesse istituzioni dell'Unione a disporre di *"un ampio numero di registri solidi e ampliati*

[13] La scalabilità è capacità della rete blockchain di gestire un numero sempre più crescente di transazioni.
[14] L'interoperabilità è la caratteristica per la quale sarebbe consentita l'interazione tra sistemi diversi tra loro, in questo caso tra diverse tipologie di blockchain.

per evitare la concentrazione dei dati nelle mani di pochi operatori del mercato" e *"invita la Commissione a collaborare con gli Stati membri"* per garantire "*la certezza del diritto […] promuovendo l'armonizzazione all'interno dell'Unione".* Per poter raggiungere questo risultato si ravvisa, inoltre, la necessità di educare la cittadinanza all'utilizzazione di queste tecnologie permettendo *"la partecipazione attiva e inclusiva […] nel cambio di paradigma"*[15] senza che l'Unione stessa disciplini le DLT, in quanto sono strumenti in continuo sviluppo, quindi risulterebbe difficile avere dei testi normativi sempre aggiornati. Sempre a livello sovranazionale sono presenti l'*EU Blockchain Observatory Forum* e l'*European Blockchain Partnership.* L'*EU Blockchain Observatory Forum* è un'iniziativa della Commissione Europea che ha come obiettivo quello di stimolare lo sviluppo e la diffusione della blockchain all'interno dell'Unione e di far sì che l'UE possa raggiungere lo status di leader globale in questo settore. La mission prevede il monitoraggio delle iniziative blockchain in Europa, la produzione di una fonte più completa possibile su di esse, la creazione di un forum per condividere opinioni ed informazioni e proporre raccomandazioni sul ruolo che l'UE potrebbe avere in questo campo[16]. L'*European Blockchain Partnership* si propone come iniziativa ad opera della Commissione Europea per lo sviluppo di infrastrutture blockchain diffuse in tutta Europa. Con questa partnership si vuole garantire una stretta collaborazione tra gli Stati membri sostenendo l'interoperabilità e l'implementazione di servizi basati su blockchain[17]. Infine, bisogna considerare anche l'EBSI, ossia l'*European Blockchain Services Infrastructure* che trae origine dall'*European Blockchain Partnership*. L'obiettivo è quello di fornire un servizio migliore in tutto il territorio europeo, conservare i dati in *"a trusted and decentralised way"* permettendo nuove forme di verificazione, tracciabilità e trasparenza. Si osserva come le imprese siano più portate a sfruttare l'EBSI[18] utilizzando le tecnologie da essa fornita, ossia (i) APIs, ovvero l'interfaccia di programmazione delle applicazioni che permette a esse di comunicare tra di loro[19], (ii) smart contracts, ossia contratti intelligenti che utilizzano un protocollo che esegue i termini di un contratto[20] e infine (iii) un database decentralizzato di informazioni a cui può accedere l'interessato per completare il business process. Il database è dotato di due gruppi di lavoro, ossia *The Blockchain Policy and Framework Conditions Working Group* per definire le condizioni politiche, legali e regolamentari ai fini della diffusione della blockchain e *The Use Cases and Transitions Scenarios Working Group,* il quale si focalizza sui casi di utilizzo della blockchain più promettenti con attenzione al settore

[15] Parlamento Europeo, 2018
[16] Per approfondimenti si veda https://www.eublockchainforum.eu/about
[17] Tratto da https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi#how-it-works
[18] Tratto da https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi
[19] Tratto da https://www.ibm.com/it-it/topics/api
[20] Smart contract, Szabo, 1994

pubblico. In sintesi si può affermare come, da un lato, vi è una certa attenzione a livello sovranazionale circa lo studio e l'applicazione della blockchain e delle DLT e le loro potenzialità, dall'altro osservando il funzionamento della blockchain emergono alcuni elementi chiave quali l'essere una tecnologia a registro distribuito in una struttura in blocchi che funziona tramite algoritmi di consenso e la crittografia di hash.

2.2. Elementi della blockchain

2.1.1. Distributed Ledger Technologies

Le DLT, acronimo per *Distributed Ledger Technologies*, sono una particolare forma di tecnologia che viene utilizzata per distribuire, scambiare o archiviare dati tra una pluralità di utenti tramite una rete che può essere pubblica o privata[21]. La rete pubblica è accessibile a chiunque, per cui è sufficiente scaricare il software. Ad esempio, i programmi di condivisione di file multimediali come UTorrent o Emule si basano su una rete peer – to – peer pubblica scaricabili direttamente da Internet. La rete privata, invece, necessita di un'autorizzazione per poter partecipare al network. Il principale obiettivo che queste tecnologie intendono perseguire è quello di eliminare la presenza di una parte terza e conseguentemente permettere ai soggetti di interagire tra loro anche in totale assenza di fiducia nella controparte[22]. Le DLT sono il punto di arrivo di una lunga evoluzione delle architetture di decentramento a partire dai cc.dd. dumb terminals e dal mainframe per poi proseguire con l'architettura server – client e il cloud computing per giungere, infine, alla tecnologia peer – to – peer. In particolare nella prima generazione, ossia la struttura formata da dumb terminals e dal mainframe, tutte le operazioni di calcolo e di elaborazione dei dati venivano concentrate nel mainframe, mentre i terminals detti dumb, ossia "stupidi", erano collegati al mainframe e funzionavano come periferiche di input e output senza la possibilità di effettuare alcun tipo di operazione[23]. Successivamente si passò all'architettura client – server, un sistema decentrato di scambio di informazioni utilizzato nella vita di tutti giorni. Per esempio, il protocollo Hypertext Transfer Protocol, conosciuto come http, permette lo scambio di informazioni in Internet. Il sistema client – server prevede principalmente due attori: il client che invia richieste e il server, ossia il database che fornisce le informazioni richieste[24]. Nello schema server – client non si è ancora in una vera e propria forma decentralizzata, in quanto i client devono necessariamente riferirsi ad un unico server, dunque, nel caso in cui ci fosse un malfunzionamento, l'intero sistema non sarebbe più in grado di funzionare. La struttura decentralizzata

[21] Farahani, Firouzi, & Luecking, 2020
[22] Diedrich, 2020
[23] El Ioini & Pahl, 2018
[24] Haroon-Sulyman, 2014

si realizza, quindi, con il cloud computing che prevede la fornitura di una serie di servizi, quali il drive per i documenti e le foto tramite l'ausilio della rete Internet. In questo sistema si pone il problema del *locked in*[25], ossia il fatto che si voglia chiudere l'utente in una determinata galassia operativa senza la possibilità di comunicare con altre galassie operative[26]. Il passo successivo che permette di avvicinarsi alle DLT e alle blockchain è la tecnologia peer – to – peer costituita da nodi che allo stesso tempo sono client e server[27]. I dati sono distribuiti tra tutti i *peers* per cui questa tecnologia funziona nel momento in cui sono presenti molti nodi attivi nella rete che permettono un accesso facilitato a nuovi partecipanti al network, i quali sono in grado di connettersi ad altri *peers.* Questo fa sì che più nodi ci sono, più aumentano le operazioni che si verificano nella rete e di conseguenza anche nel caso in cui un gran numero di nodi dovesse abbandonare il network esso continuerebbe, comunque, ad operare. Spesso le DLT vengono confuse con le blockchain, ma sono due concetti diversi in quanto le blockchain sono una tipologia di DLT e non viceversa. Nel nostro ordinamento è presente una definizione di DLT fornita dall'art.8-ter del d.l. n.135/2018, il cc.dd. Decreto Semplificazioni, convertito nella legge n.12/2019. Il primo comma dispone: "*Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili"*[28]. Il Legislatore, quindi, ha dato una definizione corretta di DLT senza cadere nell'equivoco di confonderle con le blockchain andando a delineare i tratti fondamentali, ossia la presenza di un registro distribuito, decentralizzato che utilizza la crittografia per consentire la convalida e l'archiviazione di dati che, una volta inseriti, non possono essere più modificati. Tali elementi si ritrovano anche nelle blockchain, in quanto esse sono una specie del genus più ampio di tecnologie a registro distribuito. Emerge, però, un dato di fatto: nonostante ci siano stati dei tentativi di regolamentare tale fenomeno non è facile fornire una disciplina in materia, in quanto vi è il rischio che il testo normativo possa con il passare del tempo e con lo sviluppo delle tecnologie risultare inadeguato per cui vi dovrebbe essere un costante intervento del Legislatore in materia. La soluzione migliore, forse, sarebbe quella di evitare di regolamentare tali fenomeni ma, piuttosto, di prevedere delle linee guida che devono essere seguite dagli operatori commerciali nonché dai privati nell'utilizzazione di tali tecnologie. Se da un lato vi è stato un

[25] Sarra, 2022
[26] Per esempio, le applicazioni di Apple funzionano al meglio nel momento in cui tutti i dispositivi utilizzati dall'utente condividono lo stesso sistema operativo, per cui affinché si possano sfruttare al meglio le potenzialità di iOS è consigliabile che l'utente abbia ogni dispositivo Apple.
[27] Hoek , Dai , Lai , & Zhang
[28] Art.8-ter d.l. n.135/2018 convertito nella l. n.12/2019.

passaggio da un'architettura centralizzata formata dal mainframe e dai dumb terminals per, poi, arrivare al massimo della decentralizzazione con le reti peer – to – peer, dall'altro bisogna considerare come questa evoluzione si rifletta anche con riferimento alle varie categorie di tecnologie a registro distribuito, in quanto, non sono presenti solo le blockchain. Le blockchain sono le DLT maggiormente conosciute e quelle più familiari al pubblico, ma accanto ad esse si possono rintracciare anche Tangle, Hashgraph e Sidechain[29]. Per quanto riguarda Tangle è un sistema sviluppato da IOTA ed è un registro di dati decentralizzato il cui meccanismo di consenso è il DAG, ossia il *Direct Acyclic Graph.* Tale DLT è un'alternativa alla blockchain e prevede la presenza di nodi, chiamati siti, i quali sono tutti collegati dalle transazioni effettuate. A differenza di blockchain, il DAG non prevede una struttura in blocchi, ma un grafico per cui partendo da qualsiasi vertice non è possibile tornare indietro percorrendo il percorso contrario. Tutti i nodi presenti possono effettuare transazioni, ma affinché la transazione avviata possa essere approvata, il nodo deve riconoscere almeno due transazioni presenti nel registro avviate da altri siti. Nel momento in cui questa operazione viene effettuata, anche la sua transazione verrà validata. Con questo modello, a differenza della blockchain la quale richiede il pagamento di una commissione per il processo di validazione, non sono presenti *transactions fees* e non è più presente la dicotomia tra nodi che creano nuove transazioni e nodi che le validano, ossia i *miners.* Il vantaggio di usare Tangle sta nel fatto che con questa DLT è possibile effettuare un numero più elevato di transazioni contemporaneamente andando, quindi, a risolvere il problema della scalabilità. Ogni nodo, infatti, deve validare due transazioni precedenti affinché la sua venga confermata e questo comporta ad aumento di partecipanti alla rete il che implica un aumento di prestazioni. Un'altra DLT è Hashgraph che è particolare per l'algoritmo di consenso utilizzato, ossia il protocollo gossip. Tale protocollo, pur avendo un nome bizzarro, è molto è evocativo del suo funzionamento, infatti nel momento in cui un nodo inizia una transazione, invia le informazioni circa quella operazione a dei nodi vicini scelti a caso. Il nodo che, poi, è venuto a conoscenza della transazione passerà l'informazione ad un altro nodo, sempre scelto a random. È come il gioco del telefono senza fili: si passa l'informazione da nodo a nodo finché tutta la rete non ne viene a conoscenza. Hashgraph, inoltre, è particolare in quanto la transazione viene approvata non tramite l'utilizzazione di un algoritmo di consenso, ma tramite una votazione elettronica: se vi è la maggioranza dei 2/3, la transazione è approvata e viene registrata in ogni nodo della rete[30]. Anche questa tipologia di DLT permette di risolvere il problema della scalabilità grazie all'utilizzazione del protocollo gossip. Un'ulteriore tipologia di DLT, infine, è Sidechain, la quale unisce la consortium blockchain per poter gestire le richieste di accesso alla catena e la blockchain

[29] El Ioini & Pahl, 2018
[30] Arslan, Sipahioğlu, Şafak, Gözütok, & Köprülü, 2021

permissioned per gestire le transazioni. Questa DLT suddivide la catena in sottogruppi e ogni sottogruppo approva solo le transazioni che gli vengono inviate. È un sistema vantaggioso soprattutto per le imprese, le quali possono decidere di condividere solo un determinato set di informazioni con una cerchia ristretta di collaboratori, oppure per celare alcune informazioni riservate che potrebbero essere sfruttate dalla concorrenza[31].

2.1.2. La tecnologia peer – to – peer

Una definizione completa della tecnologia peer – to – peer è data da Rudinger Schollmeir il quale la definisce come "*A distributed network architecture may be called a Peer-to-Peer network, the participants share a part of their own hardware resources […]. These shared resources are necessary to provide the Service and content offered by the network […]: they are accessible by other peers directly, without passing intermediary entities. The participants of such a network are thus resource (Service and content) providers as well as resource"*[32]. Da questa definizione si possono trarre gli elementi chiave della tecnologia P2P, ossia si tratta di una DLT, ovvero di una tecnologia a registro distribuito, in cui i partecipanti alla rete condividono una parte delle loro capacità hardware necessarie per la fornitura del servizio che si intende offrire, come ad esempio il trasferimento e il download di contenuti multimediali. L'accesso alla rete è libero, per cui chiunque può entrare a far parte del network condividendo le proprie risorse senza la necessità di un intermediario. Si comprende, dunque, come nella rete P2P i nodi agiscono contemporaneamente da client e da server. La rete funziona nel momento in cui ogni nodo mette a disposizione le proprie risorse, in gergo *seeding*, perché altrimenti se fosse possibile solo il download dei file la rete non fornirebbe alcun tipo di vantaggio ulteriore rispetto al modello server – client[33]. Dal momento che i nodi nella rete possono essere centinaia, se non migliaia, è necessario comprendere come facciano a "vedersi". In questo caso sono presenti due tipologie di reti che i nodi possono formare, ossia una rete non strutturata e una rete strutturata. La prima prevede l'assenza di uno schema ben preciso da seguire, dunque, i nodi formano delle connessioni a random tra di loro. Non essendoci una struttura, sono delle reti molto facili da costruire, ma comportano lo svantaggio di rendere difficile la ricerca di uno specifico file all'interno della rete essendo disperso in un numero di nodi non ben definiti. La seconda, per contro, è più organizzata in quanto prevede uno schema che i nodi devono seguire[34]. L'utilizzo di tale architettura è vantaggiosa sotto diversi punti di vista, in quanto non necessita l'uso di macchine con elevate capacità di calcolo, infatti ogni partecipante alla rete utilizza il proprio computer come risorsa e non vi è nemmeno la necessità di

[31] El Ioini & Pahl, 2018
[32] Schollmeier, 2001
[33] HTTPS://WWW.MAKEUSEOF.COM/TAG/P2P-PEER-PEER-FILE-SHARING-WORKS/
[34] Innocent, 2018

essere dotati di uno specifico know-how per poter utilizzare con facilità i software che si basano sul sistema in questione. La rete peer – to - peer può essere pura, ossia si tratta di una tecnologia decentralizzata tale per cui oltre ad esserci un network formato da un numero indefinito di nodi, il network continua a funzionare se uno o più nodi dovessero essere rimossi dalla rete. Vi è poi una rete cc.dd. ibrida, in quanto priva dell'elemento della decentralizzazione, ossia è sempre presente un'autorità centrale che gestisce il flusso di dati presente nel network[35]. L'utilizzazione della tecnologia peer – to – peer è molto comune, soprattutto nel campo della pirateria e dello scambio di file multimediali. Il caso più celebre è Napster, programma di condivisione di file mp.3 creato nel 1999 da Shawn Fanning e Sean Parker. Napster fu alla ribalta in quegli anni per una serie di ragioni. Prima di tutto, è stato il primo software dedito alla condivisione di file multimediali ad utilizzare la tecnologia peer – to – peer. Tale programma è stato, per così dire, il precursore di software che hanno avuto successo nel campo della pirateria, come UTorrent ed Emule. La seconda ragione per cui Napster fu importante è che per la prima volta si parlò di diritto d'autore, in quanto vi fu una causa intentata dalla Riaa, ossia *Record Industry Association of America*[36]*,* e successivamente dal gruppo metal statunitense Metallica, i quali accusarono il programma di aver diffuso la loro canzone inedita "*I Disappear"* prima che fosse pubblicata[37]. Le accuse si basavano principalmente sul fatto che il software diffondesse il messaggio per cui la musica deve essere libera e gratuita, in quanto facilmente scaricabile da Internet per cui non ci sarebbero più stati appassionati a girovagare per i negozi di dischi e a fare acquisiti e le vendite, conseguentemente, sarebbero crollate. Questa vicenda giudiziaria portò alla chiusura del programma nel 2001. Per gioco del destino, uno dei fondatori, investì nel 2010 15 milioni di dollari in Spotify, programma di condivisione di file musicali e podcast a gratis e a pagamento[38]. La differenza è che Spotify supporta gli artisti, invece Napster metteva "in vetrina" i file scaricabili senza dare alcun tipo di contributo all'artista educando le nuove generazioni alla convinzione che l'intrattenimento dovesse essere libero e gratuito. L'utilizzo di tale struttura, ad oggi, è famosa non tanto per il download di file ma per le blockchain, le quali utilizzano questa tecnologia per il proprio funzionamento.

[35] Schollmeier, 2002
[36] Associazione dei produttori discografici statunitensi
[37] HTTPS://WWW.WIRED.IT/PLAY/MUSICA/2014/06/03/LA-STORIA-DI-NAPSTER
[38] Si veda per informazioni sulla biografia https://www.britannica.com/money/Sean-Parker

2.2.3. La struttura in blocchi

Blockchain letteralmente significa catena di blocchi, ed infatti, i blocchi sono uno degli elementi portanti di questa tecnologia. Ogni blocco è formato da due elementi: il *block header*, ossia l'intestazione e il *block data*, ossia è quella parte del blocco contenente la lista delle transazioni che sono state effettuate e la transazione stessa[39]. La parte più importante del blocco è l'intestazione in quanto composta da una molteplicità di elementi tra cui: il *block version,* il *Merkle Tree root hash,* il *nonce,* gli *nBits,* l'hash del blocco precedente e, infine, il marcatore temporale. Si intuisce come la struttura dei blocchi stessi sia molto articolata. Ogni elemento dell'intestazione ha una propria funzione. Il primo componente ha un nome che è un falso amico, in quanto *version* non deve essere inteso come "versione", ma come un set di regole di autenticazione della rete che tutti i nodi devono seguire. Sono, quindi, le regole base di funzionamento della catena. L'albero di Merkle[40] è ciò che dà la struttura al blocco stesso: può essere immaginato come un diagramma ad albero con un blocco centrale dal quale discendono una serie di rami. Questo schema viene utilizzato per archiviare un singolo valore di hash, cc.dd. *hash value*, per tutte le transazioni che vengono effettuate. L'*hash value* è contenuto all'interno di ciascuna "foglia" dell'albero di Merkle. Vi è, poi, il *nonce*, acronimo per *number used only once,* ovvero un numero che può essere utilizzato una volta soltanto. È un numero che il minatore, ossia il nodo appositamente adibito per il processo di validazione del blocco, deve scoprire per poter poi inserire il blocco nella catena[41]. Il *nonce* viene rintracciato nel momento in cui il *miner* deve risolvere un problema matematico. È uno strumento importante in quanto garantisce, in un certo qual modo, la sicurezza[42] della blockchain poiché i problemi matematici che il *miner* deve risolvere richiedono enormi capacità di calcolo e questo aiuta a scremare i nodi che potrebbero essere malintenzionati o comunque dotati di scarse capacità computazionali che rallenterebbero il funzionamento e l'accrescimento della catena. Vi sono, poi, gli *nBits* che permettono di individuare la difficoltà di creazione del blocco, e infine l'hash del blocco precedente, il quale permette la creazione della catena e il marcatore temporale che individua la data, l'ora e il giorno in cui la transazione è stata effettuata. Per quanto riguarda il procedimento[43] della creazione dei blocchi esso è piuttosto complicato e prevede una serie di fasi. Il primo passo è l'invio di un *token*, ossia degli asset che possono

[39] Namasudra & Akkaya, 2023
[40] È una struttura di dati basata su hash usata nella crittografia e nell'informatica. Essendo una struttura ad albero binario ogni nodo può generare al massimo due nodi figli. Tratto da https://www.bitpanda.com/academy/it/lezioni/tutto-quello-che-devi-sapere-sugli-alberi-di-merkle/
[41] Questo se si utilizza come algoritmo di consenso il Proof – of – Work (PoW)
[42] https://it.kamiltaylan.blog/nonce/
[43] Namasudra & Akkaya, 2023

essere tangibili, ad esempio beni materiali oppure intangibili, come diritti di voto o licenze[44], da parte di un nodo della rete che intende cominciare una transazione. Successivamente si passa al trasferimento della transazione eseguita in un pool di transazioni non confermate, le quali, poi, verranno selezionate da un miner. Il miner, quindi, risolve il problema matematico fornito dall'algoritmo di consenso della blockchain e una volta effettuato il procedimento di validazione lo registra nel *ledger* con l'aggiunta della firma digitale. Si è giunti quasi alla conclusione della formazione del blocco: una volta risolto il problema computazionale e ottenuta la firma, la transazione viene aggiunta al blocco successivo e gli altri nodi della catena verificano l'autenticità della procedura di validazione. Una volta effettuata tale operazione, i miner confermano il blocco ed esso viene aggiunto alla catena. Il legame tra il nuovo blocco e quello precedente è rappresentato dalla stringa di hash, la quale funge da catena tra un blocco e l'altro.

2.2.4. Gli algoritmi di consenso

Un'ulteriore elemento portante della blockchain è l'algoritmo di consenso detto anche protocollo di consenso. L'algoritmo di consenso permette di definire i criteri che devono essere rispettati nella blockchain per poter raggiungere un accordo tra tutti i nodi della rete al momento della creazione e della validazione di un nuovo blocco[45]. Il problema che tali algoritmi affrontano è quello di instaurare un rapporto di fiducia tra i nodi della rete, in quanto non si sa quali siano onesti e quali, invece, siano malevoli e intenzionati a compiere delle operazioni a danno della catena stessa. Gli algoritmi di consenso si suddividono principalmente in tre categorie. In primis, vi sono i protocolli *compute – intensive* come il Proof – of – Work che prevedono un elevato consumo di energia per la risoluzione di puzzle e problemi computazionali sfruttando la potenza di calcolo dell'hardware. Vi sono, poi, i *capability based protocols,* vale a dire algoritmi di consenso che selezionano un minatore in base a diversi fattori quali l'ammontare di criptovalute accantonate, come nel caso del Proof – of – Stake. Infine, nell'ultima categoria vi rientrano i *voting based protocols* i quali tramite vari sistemi di voto eleggono un *miner* che sarà adibito alla creazione del nuovo blocco[46]. Un aspetto da non sottovalutare è la possibilità che la blockchain possa essere sotto attacco, in quando vi sono dei nodi malevoli nella catena che raggirano, per così dire, l'algoritmo. La resistenza della catena, infatti, dipende dalla capacità di resistere ai cyberattacchi da parte del protocollo di consenso. Gli attacchi più comuni sono il c.d. double spending, il 51% attack e il c.d. Sybil attack[47]. Per quanto riguarda il problema del double

[44]https://www.gemini.com/it-it/cryptopedia/what-is-tokenization-definition-crypto-token#section-the-benefits-of-tokenization
[45] Ul Abadin & Haider Syed , 7th July 2021
[46] Shifferaw & Lemma, July 2021
[47] Mojtaba , Bamakan , Motavali, & Babei Bondarti , 13th April 2020

spending è ciò che ha ispirato Nakamoto nella creazione del Bitcoin. Il double spending si verifica nel momento in cui un soggetto cerca di spendere un certo ammontare di denaro nella stessa rete per due volte. All'inizio si effettua una prima transazione, la quale viene approvata e il nuovo blocco viene aggiunto alla catena. Successivamente, l'utente malintenzionato cerca di includere un nuovo blocco creando una seconda transazione che sarà fraudolenta, in quanto tenta di spendere la stessa moneta per compiere una nuova operazione. In questo modo, nel caso in cui un nuovo ramo della catena dovesse essere creato, ed è il caso della transazione fraudolenta, l'utente malevolo cercherebbe di inserirlo nella catena alterandone il funzionamento[48]. Il secondo attacco più comune è il 51% attack, il quale non è possibile evitare del tutto. Si verifica quando un utente è in grado di controllare più del 50% della rete, quindi può effettuare operazioni come il double spending o impedire ad altri nodi della rete di ricevere transazioni oneste[49]. Infine, vi è il Sybil Attack che si verifica nel momento in cui l'utente crea una serie di identità fraudolente all'interno della blockchain. Queste identità all'apparenza sono user singoli, in realtà sono controllate da un unico soggetto. Non è un attacco facile da prevenire, ma sono presenti alcuni rimedi come l'aumento del prezzo per la creazione di un nuovo blocco nella catena. Il problema di questa soluzione sta nel trovare un prezzo che sia abbordabile per l'utente medio che vuole partecipare alla rete, ma che allo stesso tempo sia in grado di prevenire questa tipologia di attacco[50]. Non esiste un numero predefinito di algoritmi di consenso, in quanto se ne possono creare sempre di nuovi che vadano a soddisfare le caratteristiche proprie della blockchain. Il numero, quindi, è potenzialmente infinito. Pur essendoci un numero indeterminato di tali protocolli di consenso, i più famosi sono il Proof – of – Work[51] e il Proof – of – Stake[52] con i relativi vantaggi, problematicità e variazioni.

2.2.4.1. Proof of Work

Il protocollo di consenso Proof – of – Work è stato teorizzato da Nakamoto nel 2008 in risposta ai c.d. *Byzantine failures,* i quali si riferiscono alla problematica di raggiungere un consenso tra i nodi distribuiti in una rete con la possibilità che siano presenti nodi malevoli. Tra gli algoritmi di consenso, infatti, oltre alle tre tipologie di cui sopra, vi è un'ulteriore distinzione che deve essere effettuata, ossia tra protocolli che supportano i *Byzantine errors*[53] e protocolli che non li sopportano. I protocolli che

[48] *Ibidem*
[49] *Ibidem*
[50] *Ibidem*
[51] Da ora sarà indicato con l'acronimo PoW
[52] Da ora sarà indicato con l'acronimo PoS
[53] È una metafora utilizzata per descrivere una strategia nella quale vi è la necessità di raggiungere un accordo per evitare il fallimento del sistema considerando il fatto che tra i partecipanti vi potrebbe essere qualche soggetto poco affidabile. Tradotto nel linguaggio informatico, questo problema consiste nel far sì che una rete di computer collegati tra di loro sia

non considerano l'eventualità per la quale nella rete siano presenti nodi malevoli sono denominati *Non Byzantine fault-tolerant protocols*, mentre i *Byzantine fault – tolerant*[54] prevedono tale evenienza. Il Proof – of – Work fa parte della categoria di algoritmi di consenso che sfruttano il potere computazionale dei nodi, ergo rientra nella categoria del *compute – intensive protocol* e prende atto che ci possano essere all'interno della catena dei nodi poco affidabili. L'idea alla base del funzionamento di tale protocollo è la risoluzione di un problema matematico. Il nodo che lo risolve per primo si guadagna la possibilità di creare un nuovo blocco, di aggiungerlo alla catena e di ricevere una ricompensa, solitamente in BTC in quanto è l'algoritmo che viene utilizzato nel Bitcoin, per il lavoro svolto. La prova del lavoro, quindi, è la soluzione di un puzzle. L'origine di questa idea risale al 1974 con i rompicapi di Merkle utilizzati come strumento per implementare chiavi pubbliche crittografate[55]. Il Proof – of - Work è utilizzato soprattutto nella prima generazione di blockchain, ossia quella teorizzata dal padre del Bitcoin, il cui funzionamento è piuttosto semplice. All'interno della rete sono presenti dei nodi cc.dd. minatori che hanno il compito di risolvere problemi matematici forniti dal protocollo di consenso affinché possano aggiungere un nuovo blocco all'interno della catena. L'obiettivo del minatore è quello di calcolare un valore random, ossia il *nonce*[56], sfruttando il proprio potere computazionale. Una volta trovato il *nonce*, questo viene confrontato con il valore di riferimento, ossia il c.d. *target value*, e se risulta essere uguale o inferiore ad esso, il problema matematico è stato risolto con successo. Una volta trasmesso il *target value* a tutti gli altri nodi della catena, essi verificano la correttezza dell'operazione. In questo modo viene creato il nuovo blocco che, a seguito della procedura di validazione, viene aggiunto alla blockchain. Non è detto che il minatore al primo tentativo riesca a risolvere il puzzle, in quanto potrebbe esserci l'eventualità per cui il *nonce* trovato e il valore di riferimento non siano uguali o che il *nonce* sia superiore al *target value*. In questo caso i *miner* continueranno ad utilizzare il loro potere computazionale e a cambiare *nonce* finché non trovano un valore corrispondente a quello di riferimento. All'interno di una blockchain che utilizza tale protocollo di consenso è chiaro come siano presenti due tipologie diverse di nodi, ossia i *full node* e gli *account*. I *full node* sono i *miners* che provvedono al funzionamento dell'algoritmo e validano le

in grado di comunicare e di raggiungere un consenso anche se alcuni di essi siano danneggiati. Tratto da: https://academy.bit2me.com/it/que-es-coinjoin/

[54] Xiong , Chen, Wu, Zhao, & Yi, 2022

[55] Questi rompicapi essenzialmente prevedono tre attori, X,Y,Z. X e Y vogliono comunicare tra di loro, mentre Z è l'avversario che vuole scoprire il contenuto del messaggio tra X e Y. X genera un N numero di puzzle che invia a Y, il quale deve risolverli. Ogni puzzle contiene due informazioni: l'ID e la chiave del puzzle, ossia una delle possibili chiavi che possono essere utilizzate per le successive comunicazioni crittografate. Y seleziona un puzzle da risolvere, una volta risolto invia l'ID a X e utilizza la puzzle key come chiave per ulteriori comunicazioni crittografate. Se Z volesse trovare la chiave che utilizzano X e Y nelle loro comunicazioni, allora dovrebbe risolvere tutti i puzzle forniti da X il che comporta un costo in termini di energia e di forza molto più elevato rispetto a quanto sostenuto da X. Per ulteriori approfondimenti si veda Merkle, 1978.

[56] Acronimo per number used only once.

transazioni. Gli *account*, invece, sono i nodi dotati di un portafoglio digitale, i quali spendono un certo ammontare di criptovaluta per effettuare transazioni, ma non hanno alcun ruolo significante nel processo di creazione e validazione del blocco[57]. Il Proof – of – work è un algoritmo relativamente semplice da implementare e garantisce una certa resilienza della catena agli attacchi, soprattutto perché più è elevato l'*hashing rate*, ossia il totale dell'*hashing power* che è il valore che individua il potere computazionale utilizzato dal minatore per risolvere il puzzle, più per un nodo malevolo sarà costoso progettare e porre in essere un attacco[58]. Se da un lato questo algoritmo proprio per la facilità di implementazione e per la sicurezza che garantisce risulta essere adottato dalla maggior parte delle blockchain, dall'altro lato bisogna considerare alcune criticità che hanno portato alcune delle blockchain più famose, prima tra tutte Ethereum, ad utilizzare il secondo protocollo di consenso più diffuso, ossia il Proof – of – Stake. Uno dei problemi del Proof – of – Work è l'elevato consumo energetico dovuto allo sfruttamento dei poteri di calcolo del nodo per risoluzione dei problemi computazionali forniti dall'algoritmo. Si stima, infatti, che il consumo energetico di Bitcoin, che ancora oggi utilizza come protocollo di consenso il Proof – of – Work, per anno sia molto vicino ai valori del consumo energetico dell'Irlanda o di Hong Kong[59]. Un'ulteriore criticità riguarda la scalabilità, ossia la possibilità per la blockchain di garantire l'efficienza e di mantenere intatte le prestazioni nel momento in cui aumenta il carico di lavoro, ossia nel momento in cui aumentano le transazioni effettuate dai minatori. Nel Bitcoin, ad esempio, vi è una transazione ogni dieci minuti e questo non è un risultato accettabile al giorno d'oggi, in quanto in una rete ogni secondo avvengono centinaia e se non migliaia di transazioni ed essa deve essere in grado di sopportare un aumento del carico di lavoro. Per ovviare al problema della scalabilità sono state studiate alcune variazioni al Proof – of – Work, la più nota tra queste è il Bitcoin – NG. Nel Bitcoin - NG il tempo è diviso in epoche. Ogni epoca ha un suo leader, il quale potrebbe essere paragonato al minatore del PoW, che ha il compito di serializzare le transazioni effettuate. Per facilitare tale operazione, il protocollo introduce due nuove categorie di blocchi, ossia i *key blocks* per la elezione del leader e i *microblocks* che detengono le voci di registro. Ogni blocco è costituito da una intestazione che contiene l'hash del blocco precedente. I *key blocks* hanno il compito di eleggere il leader, ossia il minatore, che provvede ad effettuare le transazioni e contiene una chiave pubblica che verrà poi utilizzata dai micro-blocchi. I *key blocks* nascono dalla risoluzione di un puzzle, come nel protocollo di consenso PoW. Vi sono poi i micro-blocchi, altro componente fondamentale di questa variante del PoW, strettamente collegati al blocco leader che è colui che li genera. Affinché un *microblock* sia valido, le voci di registro e la firma

[57] Lepore , et al., 2020
[58] Ul Abadin & Haider Syed , 7th July 2021
[59] Lepore , et al., 2020

digitale devono essere valide. Un micro-blocco è, quindi, invalido nel momento in cui il marcatore temporale non è nell'immediato presente[60]. Ad esempio, se il marcatore temporale dovesse indicare come data e ora il 10 aprile 2024 ore 12:00 a.m. e non la data e l'ora in cui la transazione è stata effettuata, il micro-blocco sarebbe invalido, in quanto nella blockchain non è possibile, a meno che non si tratti di una blockchain che sfrutta gli smart contract, sfruttare il marcatore temporale ponendo come condizione che la transazione avvenga in un momento successivo. Un esempio di come queste criticità abbiano fatto sì che ci fosse il passaggio da tale algoritmo di consenso al Proof – of – Stake è Ethereum, nota blockchain creata nel 2013 da Vitalik Buterin. Ehtereum si differenzia rispetto alla blockchain creata da Nakamoto, in quanto non permette solo lo scambio di denaro, ma permette di effettuare tale operazione apponendo delle condizioni e di programmare creando delle applicazioni decentralizzate sulla rete sfruttando gli smart contracts. Questo passaggio è avvenuto solo nel 2022, infatti prima Ethereum sfruttava il Proof – of – Work.

2.2.4.2. Proof – of – Stake

Il Proof – of – Stake è il secondo algoritmo di consenso maggiormente utilizzato nelle reti blockchain lanciato per la prima volta nel 2012 da Peercoin, moneta digitale antagonista di Bitcoin, come alternativa al Proof – of – Work. A differenza del PoW, nel Proof – of – Stake non si considera il fattore lavoro, ma il fattore tempo vale a dire che gli utenti che hanno per il maggior tempo possibile accantonato una certa soglia di monete sono coloro hanno maggiori possibilità di essere scelti per la creazione di nuovi blocchi. In questo caso non vi è alcun problema matematico da risolvere, il tutto si basa su quanto patrimonio si ha a propria disposizione. Nel Proof – of – Stake i minatori vengono chiamati *forger* e il processo di *mining* è detto *forging*[61]. All'inizio, ogni nodo deposita un certo ammontare di monete, detto *stake*, e tale deposito viene utilizzato dall'algoritmo per selezionare il prossimo *forger*. L'individuazione del *forger* può avvenire tramite due meccanismi di selezione, ossia il *coin age selection* e il *randomized block selection.* Per quanto riguarda il *coin age,* tale valore viene calcolato moltiplicando il numero totale delle monete accantonate dall'utente per il numero di giorni in cui le monete sono state trattenute. Ad esempio se X ha 30 monete trattenute per 10 giorni, il suo *coin age* sarà di 300. In questo metodo di selezione sono presenti un minimo e un massimo di detenzione dello *stake* corrispondenti a 30 giorni e a 90 giorni[62]. Questo minimo e massimo sono previsti per evitare che qualche utente malintenzionato aumenti la probabilità di essere scelto come *forger* trattenendo lo *stake* per un lungo periodo di tempo in modo da avere un *coin age* elevato. Il

[60] Eyal, Gencer, Gun Sirer, & van Renesse, 2016
[61] Shifferaw & Lemma, July 2021
[62] *Ibidem*

secondo meccanismo di selezione è il *randomized block selection*[63]*,* ossia un *forger* dotato di uno specifico *hit value* viene selezionato per la creazione del prossimo blocco. L'*hit value* viene calcolato dal *forger* tramite la sua chiave privata crittografando l'hash del blocco precedente. Se tale valore è inferiore al valore di riferimento, il nodo in questione viene selezionato per il processo di creazione e validazione del blocco.

Il Proof – of – Stake venne sviluppato come alternativa al Proof – of – Work, in quanto basandosi sull'ammontare di monete accantonate, i nodi non devono risolvere alcun problema matematico e questo permette di far fronte alle due problematiche principali del PoW, ossia l'elevato dispendio energetico e la scalabilità. Generalmente ogni algoritmo di consenso presenta delle criticità, in quanto non esiste un protocollo perfetto, ma a misura delle esigenze della blockchain stessa. Per tale ragione, anche il Proof – of – Stake presenta alcuni svantaggi, principalmente due. Il primo problema è il concetto del *"*i ricchi diventano sempre più ricchi*"*, vale a dire che il Proof – of - Stake è un protocollo che favorirebbe chi ha già un certo ammontare di monete accantonate[64]. Coloro che hanno un certo asset hanno maggiori probabilità di essere selezionati come nodi creatori di nuovi blocchi da aggiungere alla catena favorendo in questo modo anche una maggior centralizzazione della catena. Il secondo problema riguarda, invece, la remota possibilità che vi sia una presenza maggiore di utenti malintenzionati, in quanto, secondo questo protocollo di consenso, i nodi che non sono stati selezionati come *forger* riacquistano il capitale accantonato[65], il che potrebbe tentare l'utente in questione a trattenere monete per un lungo periodo di tempo aumentando, quindi, il proprio *coin age*. Questa seconda criticità è meno preoccupante, in quanto il Proof – of – Stake garantisce un certo livello di sicurezza della blockchain, infatti per poter attaccare la catena l'utente deve detenere più del 50% dello *stake* in totale per poter manipolare la catena[66], dando vita ad un 51% attack, e questo richiede un elevato dispendio di risorse che non tutti possono permettersi. Al di là delle problematiche che ogni algoritmo di consenso pone, un esempio concreto di applicazione del Proof – of – Stake è la blockchain Ethereum. Ethereum fino al 2022 utilizzava il Proof – of – Work, ma a seguito dei limiti che esso pone il Proof – of – Stake è l'algoritmo di consenso da allora utilizzato. Ethereum è una blockchain che si basa sugli smart contract la quale permette scambi di denaro tra gli utenti della rete e la creazione di applicazioni decentralizzate dette DApps. La moneta di scambio è l'Ether[67] ed è ciò che permette all'utente di partecipare come validatore depositando 32 ETH corrispondenti a sessantamila novecento

[63] *Ibidem*
[64] *Ibidem*
[65] *Ibidem*
[66] https://thecryptogateway.it/proof-of-stake/
[67] Abbreviato a ETH

sessantuno euro e sessantadue centesimi[68]. Questo è l'ammontare di capitale minimo che chiunque intenda partecipare alla rete deve immettere in uno smart contract. In Ethereum la transazione avviene seguendo una serie di passaggi. L'utente crea e firma una transazione con la propria chiave privata. Successivamente la transazione viene inviata ad un client di esecuzione della blockchain che ha lo scopo di verificarne la validità. Una volta che la transazione è valida, essa viene aggiunta all'elenco delle transazioni in sospeso e trasmessa agli altri nodi nella rete. Quando essi la ricevono, la aggiungono al proprio elenco di transazioni in sospeso.

In Ethereum i nodi che formeranno i nuovi blocchi della rete vengono selezionati con RANDAO, ossia un algoritmo che seleziona i nodi della rete in modo casuale combinando "*un hash dal propositore di blocchi con un seed aggiornato ad ogni blocco"*[69]. Una volta creato il blocco, esso viene trasmesso agli altri nodi, i quali tramite il loro client di validazione attestano che il blocco è valido e che "*è il blocco successivo logico nella sua visione della catena"*[70] e viene aggiunto alla blockchain concludendo, così, il processo di validazione. Questo è un esempio di come il Proof – of – Stake viene concretamente attuato, ma nel mondo dei protocolli di consenso sono presenti una serie di varianti, la più conosciuta e diffusa è il Delegated Proof – of – Stake, in acronimo DPoS.

Il Delegated Proof – of – Stake, creato da Daniel Larimer nel 2014, è una evoluzione del Proof – of - Stake ed è un protocollo di consenso appartenente alla categoria dei *voting based protocols.* Il meccanismo di tale algoritmo di consenso è molto semplice. Esso si basa sul Proof – of – Stake, per cui sono sempre presenti utenti dotati di un certo ammontare di capitale. La novità di tale algoritmo riguarda la possibilità per gli utenti di eleggere i loro rappresentanti, chiamati delegati o testimoni, affinché essi procedano con la creazione e la validazione dei blocchi. Si può affermare come con tale protocollo di consenso si sia teorizzato per la prima volta un meccanismo di democrazia rappresentativa all'interno della blockchain. La modalità di votazione non è unica, infatti il processo decisionale differisce a seconda della tipologia di blockchain che utilizza tale protocollo di consenso. In generale, però, nella maggior parte delle blockchain in cui si utilizza il Delegated Proof – of – Stake gli utenti procedono con una votazione diretta dei loro rappresentanti oppure delegano il loro diritto di voto ad un altro utente parte della catena[71]. È un'alternativa che pone dei vantaggi rispetto al Proof – of- Stake in termini di scalabilità delle transazioni e del consumo energetico[72], ma pone delle problematicità, poiché è un algoritmo che rende la rete più centralizzata concentrando nelle mani di

[68] 1 ETH corrisponde a 1915.06€, valore in data 12 novembre 2023
[69] Ethereum
[70] *Ibidem*

[71] Tratto da https://101blockchains.com/delegated-proof-of-stake-dpos/

[72] Mojtaba , Bamakan , Motavali, & Babei Bondarti , 13th April 2020

pochi utenti la possibilità di scegliere quali siano i nodi più adatti alla creazione di un nuovo blocco aumentando, conseguentemente, il rischio che la rete venga sottoposta ai c.d. 51% attack.

2.2.5. Le funzioni di hash

Le funzioni di hash sono un ulteriore elemento chiave delle blockchain, in quanto, grazie alle loro proprietà garantiscono un elevato livello di sicurezza della catena. Le funzioni di hash sono delle funzioni matematiche che vengono utilizzate specialmente nella campo della crittografia e sono in grado di generare da un qualsiasi input, che può essere un testo, una serie di numeri, dati e quant'altro, un output di una lunghezza ben definita, ossia la stringa di hash. Il valore che risulta dalla funzione di hash viene chiamato *hash value* o *digest.* Una delle principali caratteristiche delle funzioni di hash consiste nel fatto che indipendentemente dalla grandezza dell'input, l'output generato sarà di una determinata lunghezza. A questo risultato si giunge perché, durante la fase di elaborazione, i dati che vengono immessi vengono *spezzettati* e portati in una lunghezza uniforme. *To hash,* infatti, significa triturare, sminuzzare. La lunghezza della stringa di hash dipende all'algoritmo utilizzato, difatti può essere di 32, 64, 128 o 256 bit[73]. Per poter garantire la sicurezza della blockchain e l'immutabilità dei dati le funzioni di hash che vengono utilizzate in questo ambito devono soddisfare alcune proprietà, tra cui la resistenza alle collisioni, la resistenza alla preimmagine e la resistenza alla seconda preimmagine. La collisione è quel fenomeno che si verifica nel momento in cui partendo da due input diversi si giunge allo stesso output. In questo caso la funzione di hash non è più sicura, in gergo è *broken*, ossia rotta. Per resistenza alle collisioni, dunque, si intende che dati due input sia molto difficile, se non impossibile, ottenere lo stesso output[74]. La seconda proprietà consiste nel fatto che non si possa risalire al dato di partenza, ossia all'input, partendo dal valore di hash finale[75]. È una proprietà che è strettamente collegata alla caratteristica principale della funzione di hash, ossia l'essere unidirezionale per cui dal valore finale non è possibile risalire al dato originale. Questa è una qualità che garantisce la sicurezza della blockchain, in quanto per poter risalire all'input è necessario effettuare un attacco di cc.dd. forza bruta, ossia un procedimento di *trial and error*, per cui chi ha intenzione di risalire al dato di partenza cerca di indovinare quale sia l'input. La terza proprietà, ossia la resistenza alla seconda preimmagine prevede che dato un input m_1 sia difficile trovare un messaggio m_2 tale per cui si abbia la stessa stringa di hash. A contrario, vuol dire che deve essere assai arduo avere lo stesso output partendo da due messaggi diversi, perciò dati m_1 e m_2 il risultato che si dovrebbe ottenere è

[73] Tratto da https://medium.com/techskill-brew/hash-functions-in-blockchain-part-3-blockchain-basics-c3a0286064b6
[74] GENÇOĞLU1, 2022
[75] *Ibidem*

hash(m_1) ≠ hash(m_2) e non hash(m_1) = hash(m_2)[76]. Queste sono le tre proprietà fondamentali che ogni funzione di hash deve rispettare per poter essere utilizzata nella blockchain, ma vi sono ulteriori caratteristiche che la definiscono. Una di esse consiste nell'essere deterministica, ossia dato un certo input, l'output sarà lo stesso. Ad esempio, se si dovesse utilizzare l'algoritmo SHA-256, impiegato nella blockchain, e scrivere "Ciao" l'output sarà sempre *25c73520e69f4bf229811e8e46ffe7d80471544b9bee15ed25044b86be4115ad*[77].

L'essere deterministica implica un'ulteriore peculiarità, ossia nel momento in cui dovesse essere cambiato un solo elemento dell'input, il risultato che si ottiene è completamente diverso. Da ciò si comprende come le funzioni di hash siano fondamentali nelle blockchain, in quanto grazie a queste prerogative la sicurezza della catena agli attacchi è garantita. Nel momento in cui la blockchain è sotto attacco, per esempio un utente malevolo ha cercato di modificare una transazione o di eliminare un blocco dalla catena, questo risulta essere immediatamente evidente, poiché la manomissione di un blocco richiede che tutti gli altri blocchi, collegati tra di loro tramite il richiamo all'hash precedente nel blocco successivo, vengano alterati. È facilmente comprensibile come un'operazione di tal portata sia davvero complicata da effettuare a causa della lunghezza della catena stessa. Ecco, dunque, come le funzioni di hash assicurano un certo livello di sicurezza all'interno della blockchain. Vi sono diverse funzioni crittografiche di hash, le più comuni e maggiormente utilizzate sono l'MD5, ossia il *Message Direct 5* e l'algoritmo SHA, acronimo per *Secure Hash Algorithm* teorizzato e messo in atto dal NIST[78]. Il Message Digest 5 è stato sviluppato da Ronald Rivest nel 1991 come evoluzione dell'algoritmo precedente, ossia l'MD4 a seguito di alcune problematicità riscontrate dovute al fatto che l'MD4 era stato creato per essere veloce, ma era sottoposto a numerosi attacchi. L'MD5 è un algoritmo più lento, ma viene sacrificata la velocità in nome della sicurezza[79]. Il funzionamento è piuttosto complesso e prevede una serie di fasi[80]. La prima consiste nell'aggiungere al messaggio di partenza dei bit, il c.d. *padding,* affinché la lunghezza sia di 448 modulo rispettando i 512 bit dei blocchi su cui opera l'algoritmo per generare messaggi di 128-bit corrispondenti a 32 caratteri[81]. Un "1" viene aggiunto al messaggio, vengono, poi, aggiunti tanti "0" quanti necessari affinché la lunghezza del messaggio sia di 448 modulo. Il secondo passaggio consiste nell'aggiungere al risultato del primo passaggio una rappresentazione in 64-bit del messaggio originario, prima delle aggiunte. A questo punto, il messaggio che risulta ha una lunghezza che corrisponde esattamente ad un multiplo di

[76] *Ibidem*
[77] https://sha256algorithm.com
[78] National Institute of Standards and Technology
[79] (Rivest, 1992)
[80] *Ibidem*
[81] Dal momento che 256-bit sono 64 caratteri, basta fare una semplice proporzione 256:64=128:x il cui risultato è 32.

512 bit con una lunghezza in caratteri di 32-bit. Il terzo passaggio prevede il processo di inizializzazione, per cui ci sono quattro blocchi da 512-bit corrispondenti ad A, B, C e D che vengono utilizzati per calcolare il valore di hash. Ogni blocco viene processato tramite una serie di operazioni matematiche. Successivamente si calcola l'hash value concatenando le quattro parole della variabile ottenuta creando un messaggio di 128-bit corrispondente a 32 caratteri. Il risultato che si ottiene è unico, difatti nell'ambiente della crittografia si utilizza il termine *fingerprint*, ossia impronta digitale per sottolineare l'unicità del valore di hash così ottenuto. Questo algoritmo di hash pur essendo piuttosto complesso nel suo funzionamento presenta una serie di vulnerabilità, tra cui il non essere sufficientemente resistente alle collisioni. Per tale ragione l'utilizzo del *Message Digest 5* fu sconsigliato e fu promossa l'utilizzazione del *Secure Hash Algorithm*[82] creato dal NIST nel 1995. Sono presenti diverse generazioni dello SHA tra cui SHA-1, SHA-2 e SHA-3. Il funzionamento dello SHA segue le stesse fasi del *Message Digest 5* teorizzato da Rivest. Si può, quindi, affermare come i *Secure Hash Algorithm* possano essere considerati come uno sviluppo ulteriore del MD5. La prima generazione, ossia lo SHA-1, produce un valore di hash di 160-bit dall'input. Lo SHA-2 è una evoluzione della prima generazione. Vi è stato questo passaggio da SHA-1 a SHA-2 a seguito di alcuni attacchi risalenti al 2005 che hanno evidenziato come tale algoritmo non sia in grado di resistere alle collisioni[83]. Il NIST, dunque, ha promosso lo sviluppo della seconda generazione di *Secure Hash Algorithm* con l'obiettivo di non adottare più lo SHA-1 entro il 31 dicembre 2030[84] prevedendo una serie di passaggi per poter raggiungere questo traguardo. In primis vi è la necessità di rendere più resistente lo SHA-2 agli attacchi a cui può essere sottoposto, considerando che sono gli stessi della generazione precedente. Per poter garantire una maggiore sicurezza dell'algoritmo in questione, inoltre, vi è la necessità di promuovere la ricerca circa lo sviluppo degli algoritmi di hash e circa la prevenzione degli attacchi[85]. Se si è in grado di comprendere come questi attacchi inficiano sull'algoritmo si è in grado di trovare i punti deboli e di porvi rimedio rendendo l'algoritmo stesso più resistente e più sicuro. Nel 2015 il NIST annunciò la nascita di SHA-3, evoluzione dello SHA-2. È il primo algoritmo che viene creato tramite una competizione aperta al pubblico facendo, quindi, una selezione tra i migliori progetti presentati provenienti da tutto il mondo[86]. Lo SHA-3 non è, però, ancora implementato del tutto. La ragione principale risiede nel fatto che al momento del lancio di SHA-3 la maggior parte delle imprese utilizzavano e utilizzano ancora l'algoritmo della generazione

[82] L'acronimo è SHA.
[83] https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1
[84] *Ibidem*
[85] Si veda nota n.83
[86] https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

precedente[87], dunque, non vi era ragione di effettuare un cambiamento di tale portata, considerando il fatto che non vi sono ancora delle evidenze sufficienti a garantire che lo SHA-3 sia sicuro e resistente agli attacchi. Per quanto riguarda le blockchain, l'algoritmo che viene adottato a partire dal Bitcoin in poi è lo SHA-256 appartenente alla famiglia del *Secure Hash Algorithm 2*. Lo SHA-256 è coinvolto nel processo di creazione e di validazione dei blocchi all'interno della rete, ossia è l'elemento chiave all'interno del processo del *mining.* Al momento lo SHA-256 è considerato come l'algoritmo più sicuro in quanto è in grado, a differenza di altri, di resistere alle collisioni.

3. Tipologie di blockchain

Se gli algoritmi di consenso che vengono eseguiti nella blockchain sono potenzialmente infiniti, in quanto possono essere creati *ad hoc* per soddisfare diverse esigenze, le tipologie di blockchain non sono infinite: esse, infatti, possono essere raggruppate in tre categorie ognuna delle quali con i propri punti di forza e di debolezza. Le tre categorie di cui si tratterà sono: blockchain *permissionless*, blockchain *permissioned* ed infine un modello ibrido, ossia le *consortium*.

3.1. Blockchain pubblica

La prima tipologia di blockchain che viene presa in considerazione è la blockchain pubblica, conosciuta anche come *permissionless*. La denominazione permette di cogliere immediatamente l'essenza di tale tipologia, ovverosia chiunque dotato di un computer e di una connessione Internet può entrare a far parte della rete senza la necessità di dover richiedere e ottenere una autorizzazione. Questo genere di blockchain viene utilizzato principalmente nelle transazioni tra più soggetti che prevedono lo scambio di moneta virtuale, come nel caso del Bitcoin o di Ethereum. Il fatto che le blockchain pubbliche non richiedano alcun tipo di permesso per poter partecipare alla rete implica una serie di caratteristiche che la rendono appetibile, oltre che per il settore delle criptovalute, anche in altri ambiti come il voto elettronico o i servizi forniti dalla sanità pubblica o previdenziali. Le caratteristiche principali che rendono questa tipologia di blockchain interessanti sono la decentralizzazione, la facilità di accesso alla rete, la trasparenza, l'immutabilità e la resistenza agli attacchi. Considerando la struttura della blockchain, ossia il fatto di essere una tipologia di tecnologia a registro distribuito, la decentralizzazione prevede l'assenza di una terza parte che coordini la rete. Questa è, invece, la caratteristica delle reti cc.dd. *permissioned*, le quali sono per lo più centralizzate in quanto è presente

[87] https://www.encryptionconsulting.com/education-center/what-is sha/#:~:text=SHA%20stands%20for%20secure%20hashing,modular%20additions%2C%20and%20compression%20functions

una parte terza che assume il ruolo di gatekeeper. Detto in altri termini, nella blockchain permissioned la parte terza permette o nega l'accesso a chi intende partecipare in base alla soddisfazione o meno di determinati requisiti. La decentralizzazione è strettamente correlata, poi, ad un'altra peculiarità: la resilienza della rete agli attacchi. Più nodi sono presenti, più la catena sarà resistente[88]. Le blockchain pubbliche, inoltre, dal momento che non prevedono alcun tipo di requisito da soddisfare per poter partecipare alla rete permettono a chiunque di farvi parte e questo comporta anche un certo grado di fiducia tra i partecipanti. Anche la fiducia risulta essere una nota distintiva delle blockchain *permissionless*, in quanto collegata alla trasparenza. Se si considera, infatti, che non è presente una parte terza che controlla la rete, i partecipanti devono in qualche modo sviluppare un certo grado di fiducia affinché non vengano compiute operazioni a danno della rete stessa. Questo implica trasparenza, dal momento che ogni operazione è tracciabile e grazie alle funzioni di hash risulta evidente ogni tentativo di manomissione. Trasparenza, dunque, nel senso di buona condotta, per cui ogni nodo sa che deve comportarsi onestamente per evitare di non fare più parte della catena e nel senso di tracciabilità delle operazioni. Strettamente collegata alla trasparenza, poi, è l'immutabilità. Per immutabilità si intende la proprietà per la quale i dati una volta inseriti all'interno del blocco non possono essere più modificati. Ogni tentativo di manomissione è immediatamente visibile, in quanto cambiando anche di poco i dati immessi cambiano automaticamente anche i valori di hash ed eventualmente la catena risulta essere spezzata[89]. Le blockchain *permissionless*, oltre a presentare queste caratteristiche, le quali comportano una massiccia utilizzazione in svariati settori, presentano anche alcuni svantaggi, tra cui la necessità di essere dotati di macchinari con un elevato potere di calcolo e problemi di sicurezza legati alla privacy e all'anonimato. Per quanto riguarda la prima criticità, affinché si raggiunga il consenso tra tutti i nodi è opportuno che i macchinari adottati per l'esecuzione dell'algoritmo di consenso siano dotati di sufficienti poteri computazionali. Questo inconveniente, però, non è così preoccupante poiché oggi sono presenti diversi protocolli che permettono di raggiungere il consenso tra tutti i nodi che non necessitano, affinché possano operare correttamente nella rete, della risoluzione di problemi matematici e puzzle particolarmente complessi. Non si esclude, poi, che in futuro vengano progettati protocolli di consenso che siano in grado di ridurre a zero l'impatto ambientale della blockchain o, comunque, di ridurlo notevolmente. Il problema che, invece, desta preoccupazione è la salvaguardia della privacy. È appurato che le blockchain

[88] Questo si verifica perché essendo una DLT i dati presenti sono archiviati presso ogni nodo, dunque, in presenza di un attacco, anche se alcuni dei nodi dovessero essere messi nella condizione per la quale non sarebbero più in grado di funzionare, sono presenti tutti gli altri che detenendo una copia dei dati permettono il funzionamento della blockchain. In sostanza, poco importa se uno o più nodi non dovessero essere più operativi, perché c'è sempre il resto della catena che fa da backup.
[89] Imetaj, Amini, & Pardalos, 2021

garantiscono l'anonimato dei partecipanti, infatti non è possibile risalire direttamente alla identità dell'autore della transazione. Se da un lato viene garantito l'anonimato, dall'altro bisogna considerare come la blockchain sia una tipologia di tecnologia a registro distribuito per cui chiunque ha la possibilità di accedervi e di ottenere informazioni circa le transazioni che sono state effettuate. Questa possibilità, certamente legata alla trasparenza della blockchain, mette a rischio la privacy poiché vi è l'eventualità per cui a seguito delle transazioni effettuate siano presenti alcuni collegamenti che permettano di risalire all'identità delle parti coinvolte o di rintracciare i pattern comportamentali degli utenti facendo una semplice analisi dei dati[90]. Un altro fattore di rischio è la cattiva gestione delle chiavi pubbliche e private[91] che fungono da password che permettono agli utenti di accedere alla blockchain e di effettuare transazioni all'interno della rete. Se l'utente non è in grado di conservarle, questo comporta all'impossibilità di accedere ai propri asset perdendo, di fatto, ogni possibilità di recupero di quanto accantonato nella blockchain. Il rischio, quindi, è quello di perdere ingenti quantità di capitale senza la possibilità di recuperarlo. La chiave privata, infatti, è unica per ogni utente ed è spesso espressa come una serie di 64 numeri e lettere. Essa garantisce un certo livello di sicurezza all'interno della blockchain, in quanto sono presenti un elevato numero di combinazioni, per cui nel caso di un attacco sarebbe davvero difficile indovinare la combinazione esatta per accedere al profilo dell'utente. Per contro, però, nel momento in cui non sono più reperibili, non è più possibile effettuare alcun tipo di operazione all'interno della rete stessa. Si sono, dunque, sviluppate alcune soluzioni per salvaguardare la privacy. Un primo approccio è il cc.dd. mixing che può essere centralizzato o decentralizzato. Si parla di mixing centralizzato quando è presente un server che funge da intermediario generando le transazioni contenenti gli input e output di tutti gli utenti partecipanti alla rete[92]. Pur garantendo l'anonimato degli utenti si pone il problema del *coin theft,* ossia del furto di monete. Tra le varie proposte presenti, CoinSwap è stato il primo metodo a risolvere tale problema. Si tratta di un servizio di coin mixing ideato da Greg Maxwell nel 2013, implementato solo nel 2020. CoinSwap è uno strumento che permette di scambiare una moneta per un'altra senza la necessità di un intermediario. Due utenti, per esempio A e B, possono scambiarsi criptovalute inviandole prima ad un indirizzo CoinSwap per poi inviarle, successivamente, all'indirizzo del destinatario[93]. Il mixing decentralizzato, invece, prevede la presenza di una terza parte fidata o *semi-trusted* per mescolare transazioni di una molteplicità di utenti in modo da non rendere collegabili gli input agli output[94]. Per esempio, CoinJoin è stato uno dei primi servizi di mixing decentralizzato teorizzato da Maxwell, autore

[90] Bayan & Banach , 4-6 May 2023
[91] *Ibidem*
[92] Li, et al., 2021
[93] Tratto da https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964
[94] Li, et al., 2021

di CoinSwap. CoinJoin prevede due utenti, Tizio e Caio che vogliono effettuare uno scambio di BTC. Tizio vuole trasferire 1 BTC dall'indirizzo A all'indirizzo B e lo stesso Caio dall'indirizzo C all'indirizzo D. Sono presenti due input, A e B, e due output C e D. CoinJoin mescola gli input e gli output cosicché vi sia una sola transazione, in tal modo una terza parte non può facilmente determinare se Tizio ha ricevuto l'output D oppure l'output C[95].

Un ulteriore approccio è lo Zero-Knowledge Proof, abbreviato in ZKP. È un protocollo di verifica interattivo che permette a una parte di provare ad un'altra che una certa affermazione sia vera senza dover rilevare dettagli o informazioni aggiuntive. Questo protocollo si sviluppa in tre fasi: *witness*, *challenge* e *response*[96]. La fase *witness*, ossia di "testimonianza" prevede un soggetto, detto *prover*, che elabora una prova che contiene la sua affermazione, ossia il suo *claim*. Questa prova viene, poi, trasmessa ad un altro soggetto, il *verifier* ossia colui che verifica la veridicità dell'affermazione del *prover*. Si passa poi alla fase della *challenge*, ossia il *verifier* pone una serie di domande. Infine, vi è la risposta alle domande del *verifier* da parte del *prover*. In questa ultima fase il verificatore può, in base alle risposte ottenute, accettare o rifiutare la prova così generata. Questo è lo schema generale di funzionamento del ZKP, mentre per quanto riguarda l'implementazione nella blockchain sono presenti otto fasi[97]. Il tutto parte da una trusted authority che genera due chiavi: quella di prova e quella di verifica. Successivamente viene generata una prova che contiene l'affermazione del prover. Il prover trasmette la prova alla blockchain. Il validatore, ossia il *verifier* invia un *verificiation task* per ottenere la prova della veridicità dell'affermazione del prover. Quando i nodi della blockchain ricevono il *task*, lo verificano. Se è valido, inviano la richiesta di verificazione al *verifier* il quale invierà una risposta entro un certo periodo di tempo. Il sesto passaggio prevede l'implementazione nella catena del *task* da parte del validatore che utilizzerà la chiave di verifica per effettuare tale operazione. Infine, se il responso contiene il messaggio di conferma che il *claim* del *prover* è vero, allora tale messaggio può essere accettato. È evidente come questa tipologia di blockchain venga utilizzata soprattutto nel mondo delle criptovalute. Un esempio di blockchain *permissionless* è la rete che supporta Bitcoin.

3.1.1. Bitcoin

Il bitcoin, teorizzato nel white – paper di Satoshi Nakamoto del 2008, è la prima criptovaluta ad essere stata messa in funzione e il primo scambio di BTC è avvenuto il 12 gennaio 2009 tra Nakamoto e Hal Finney[98]. A febbraio 2011 un bitcoin equivaleva a un dollaro. Ad oggi, per acquistare 1 BTC è

[95] https://academy.bit2me.com/it/que-es-coinjoin/
[96] Sun, et al., 2021
[97] *Ibidem*
[98] Tratto da https://medium.com/thedarkside/how-bitcoin-works-everything-you-need-to-know-8442f0c8627f

necessario fare un investimento di 34.737,22 €[99]. Non è facile dare una definizione di criptovaluta, a tal proposito si può considerare quella fornita dall'opinion dell'European Banking Authority del luglio 2014. L'EBA descrive le monete vrituali *"as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically"*[100]. Questa definizione è completa individuando le principali caratteristiche della moneta virtuale, ossia (i) l'essere una rappresentazione digitale, (ii) la mancanza di un soggetto terzo che funge da intermediario come una banca o una autorità pubblica, (iii) l'essere utilizzata da persone fisiche o giuridiche come strumento di scambio per l'acquisto di beni e servizi, e infine (iv) la possibilità di essere trasferita, immagazzinata o scambiata elettronicamente. Tutte qualità queste presenti nel Bitcoin e in generale in tutte le monete virtuali ad oggi esistenti. A livello normativo, invece, sono presenti principalmente due fonti sovranazionali: la direttiva 2009/110/CE attuata nel nostro ordinamento con il d.lgs. n. 45/2012 e la direttiva n.243/2018 del Parlamento Europeo e del Consiglio. Per quanto riguarda la direttiva del 2009 sono rilevanti i considerando n.7 e n.8 in quanto affermano come la definizione di moneta elettronica debba essere tecnicamente neutra e di come debba essere generale in modo da *"non ostacolare l'innovazione tecnologica e da includere non soltanto tutti i prodotti di moneta elettronica disponibili oggi […], ma anche i prodotti che potrebbero essere sviluppati in futuro"*[101]. Si comprende come già nel 2009 vi era consapevolezza da parte delle istituzioni europee dell'opportunità di sviluppo di nuove tecnologie che permettessero uno scambio di valuta elettronica. Correndo, poi, l'anno 2009 si è a poca distanza dalla teorizzazione del Bitcoin da parte di Nakamoto. La direttiva n.243/2018, invece, pone l'attenzione sulla differenza tra moneta elettronica, come definita dall'art.2 della direttiva del 2009[102] e valuta virtuale la quale viene definita come *"una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente"*[103]. La definizione, seppur arricchita di qualche elemento quale (i) il non

[99] Valore corrispondente in data 28 novembre 2023.
[100] (EBA, 2014)
[101] (Direttiva 2009/110/CE del Parlamento europeo e del Consiglio concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/4, 2009)
[102] Articolo 2 Direttiva 2009/110/CE: "*Ai fini della presente direttiva si intende per "moneta elettronica", il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento […] che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica".*
[103] Articolo 1 Direttiva n.243/2018

essere legata a una valuta legalmente istituita e (ii) il non possedere lo status giuridico di moneta, riecheggia la definizione data dall'EBA nel 2014.

Essendo una moneta virtuale non è possibile avere tra le mani il Bitcoin. Esso, come tutte le cripto, è caratterizzato dal fatto che lo scambio avviene in una blockchain. L'obiettivo di Nakamoto con la teorizzazione di questa tecnologia era quello di risolvere due ordini di problemi: la fiducia in una parte terza ideando un sistema che permettesse a due o più persone di scambiarsi moneta senza la necessità di un intermediario considerando la fiducia come elemento debole del sistema. Inoltre si evita il double spending, situazione per la quale un soggetto spende una moneta per avviare una transazione e successivamente spende la stessa moneta per avviare una seconda transazione, fraudolenta, nella speranza che il registro riconosca la seconda operazione e non la prima. Venendo al punto focale, ossia il funzionamento di tale moneta virtuale esso è piuttosto semplice. Per effettuare un passaggio di Bitcoin da un utente all'altro è necessario che avvenga una transazione. È importante che prima della transazione vera e propria gli utenti siano dotati di un *wallet*, ossia di un portafoglio virtuale nel quale vengono conservati i Bitcoin acquistati. I portafogli elettronici, dunque, detengono le chiavi pubbliche e private le quali permettono all'utente di accedere alla rete blockchain. I wallet si distinguono in *hot wallets* e *cold wallets*[104]. La transazione ha inizio con il processo di *mining*, ossia alcuni nodi della rete blockchain, sfruttando il loro potere di calcolo, hanno il compito di risolvere complicati puzzle matematici eseguendo, quindi, l'algoritmo Proof – of – Work. Una volta risolto il problema matematico, il valore così trovato, ossia il *nonce*, viene trasmesso a tutta la rete. Gli altri nodi provvedono al controllo circa la validità della transazione. Se la transazione è valida, allora il nuovo blocco viene aggiunto alla rete e viene, quindi, creato il Bitcoin. Si deve considerare, poi, un ulteriore elemento: il Bitcoin non è una fonte inesauribile, infatti è previsto un numero limite di Bitcoin che possono essere estratti, ovvero 21 milioni[105]. Secondo le previsioni entro il 2140 non sarà più possibile estrarre Bitcoin. Il Bitcoin si basa su una blockchain pubblica, per cui chiunque dotato di una connessione Internet e un software e hardware sufficientemente potenti può far parte della rete. Si sono già discussi i vantaggi attinenti alla utilizzazione della blockchain pubblica, ma se ne possono rinvenire di altri strettamente collegati all'utilizzazione del Bitcoin. Tra questi, sicuramente il fatto di essere collegati a Internet permette di effettuare scambi, ritirare i propri Bitcoin o sfruttarli per acquistare

[104] I primi operano online e si suddividono in (i) applicazioni desktop, (ii) portafogli online e (iii) applicazioni su mobile. I secondi, invece, sono più sicuri in quanto non operano online e sono di due tipi: *paper wallets*, letteralmente "portafogli di carta", quindi i codici delle chiavi pubbliche e private vengono scritti su supporto cartaceo e hardware wallets, ossia archiviano le chiavi pubbliche e private, ad esempio, su chiavette USB o, in generale, su supporti esterni. Pur essendo più sicuri rispetto agli hot wallets, in quanto non sono sottoposti ad attacchi informatici poiché sono offline, presentano comunque qualche rischio dovuto, principalmente, alla presenza di fattori esterni quali smarrimento o eventi atmosferici che vanno a danneggiare il supporto sul quale è iscritta la coppia di chiavi. Tratto da https://101blockchains.com/crypto-wallets.

[105] Tratto da (https://medium.com/thedarkside/how-bitcoin-works-everything-you-need-to-know-8442f0c8627f

beni o servizi in qualsiasi momento, da qualsiasi luogo e in un tempo relativamente breve. È possibile, quindi, effettuare transazioni 24 ore su 24, sette giorni su sette. Inoltre una certa sicurezza delle rete tramite l'uso della crittografia e l'algoritmo SHA-256 per la validazione delle transazioni. Questo fa sì che la catena sia immutabile e che i dati immessi non possano essere modificati. Questo aspetto, però, è anche negativo in un certo senso. Se le parti avessero intenzione di modificare la transazione effettuata, dovrebbero crearne una di nuova e questo comporta l'iniziazione di un nuovo iter di creazione e validazione dei blocchi. Considerando gli svantaggi del Bitcoin e della rete blockchain vi è da valutare la possibilità per cui la rete possa essere sotto attacco, per esempio il 51% attack o il Sybil attack, nonché il fatto che ancora oggi non è presente una regolamentazione in termini generali sul funzionamento e sull'utilizzazione di tali tecnologie.

3.2. Blockchain privata

La seconda tipologia di blockchain di cui si deve tenere conto è la blockchain privata, detta altrimenti *permissioned*. Anche in questo caso l'aggettivo permette di cogliere l'essenza della blockchain in questione: per poter partecipare alla rete è necessario aver ottenuto un'autorizzazione da parte di una autorità specifica a ciò preposta[106]. La parte terza, quindi, è presente in questo modello e funge da *gatekeeper*, ossia consente o nega l'accesso in base alla soddisfazione di determinati criteri richiesti dalla blockchain stessa. Non tutti, quindi, possono partecipare alla rete. Si coglie, dunque, fin da subito una prima differenza rispetto alle blockchain *permissionless*, le quali, invece, non richiedono alcun tipo di autorizzazione per potervi partecipare: è sufficiente essere dotati di una buona connessione Internet e di un computer sufficientemente potente per potervi accedere. La rete *permissioned*, invece, può aumentare o restringere il numero di partecipanti. Questo implica una serie di conseguenze che consentono di individuare le specificità della blockchain privata. Essendo presente un numero ristretto di partecipanti questo fattore può essere sia negativo sia positivo. È negativo, in quanto vi è un numero ristretto di nodi e questo comporta delle problematicità circa la sicurezza della rete stessa, la quale è maggiormente soggetta ad attacchi. Ad esempio i cc.dd. 51% attack sono più frequenti in questa tipologia di blockchain rispetto alla blockchain *permissionless*. L'essere in pochi partecipanti, però, comporta contemporaneamente un maggior grado di fiducia tra le parti, mentre nelle blockchain *permissionless* è presente, ma in misura minore. Nelle blockchain *permissioned*, invece, la fiducia è un elemento portante. Questo fa sì che in base al grado di fiducia tra le parti, si possano autorizzare solo certi soggetti della rete ad effettuare transazioni, e quindi, aggiungere blocchi alla catena a

[106] Yaga, Mell, Roby, & Scarfone, 2018

discapito di altri[107]. La fiducia, poi, è strettamente correlata alla trasparenza condividendo, quindi, questo aspetto con le blockchain pubbliche. Essendo presenti pochi nodi, qualsiasi tentativo di manomissione del network o di coalizzazione con altri nodi per eseguire operazioni malevoli è immediatamente visibile e non tarda ad arrivare la "punizione" da parte dell'autorità di controllo, ossia l'essere definitivamente rimossi, in gergo *bannati.* La presenza di una parte terza che decide chi può entrare e chi, invece, a causa della sua cattiva condotta debba essere eliminato implica anche una centralizzazione del sistema. Le blockchain *permissioned*, dunque, si pongono in netto contrasto con l'idea originale della blockchain, ovvero l'essere una tecnologia a registro distribuito che permetta lo svolgimento di diverse tipologie di operazioni in assenza di una parte terza che funga da intermediario. In questi termini sembrerebbe, dunque, che le blockchain private siano prive dell'elemento della decentralizzazione. In realtà, facendo parte del genus più ampio delle DLT condividono con esse tale caratteristica, l'unico elemento mancante, per così dire, è la parità tra nodi in quanto alcuni hanno il potere di decidere chi far entrare e chi escludere dalla catena rispetto ad altri venendosi a creare, di conseguenza, una situazione di disparità. Il fatto che vi siano pochi nodi permette alla blockchain di effettuare transazioni in tempi molto più rapidi[108] rispetto alle blockchain pubbliche e, quindi, di essere più efficiente. Questo perché, essenzialmente, il consenso all'interno del network viene raggiunto molto più facilmente rispetto ad una rete fortemente decentralizzata e distribuita. Inoltre, la presenza di una autorità terza permette di instaurare all'interno della blockchain una sorta di governance, facendo sì che ogni nodo sia consapevole del proprio ruolo all'interno della catena. La presenza di una parte terza che gestisce l'apparato in sé e per sé non deve essere visto come un elemento negativo, perché permette una miglior organizzazione ed efficienza della blockchain. Bisogna, però, porre l'accento su un aspetto poco considerato: l'autorità terza che gestisce la rete è dotata di poteri, per così dire, assoluti potendoli esercitare anche in negativo con una funzione di censura. Funzione di censura intesa nel senso che alla prima avvisaglia di un comportamento scorretto da parte di uno o più nodi del network, essi vengono eliminati senza la possibilità di potervi fare nuovamente parte. È evidente come questa tipologia di blockchain, pur avendo qualche lato oscuro, sia molto appetibile non tanto nel contesto dello scambio di criptovalute o della fornitura di servizi, ma nel contesto del business to business. Le imprese utilizzano questa forma di blockchain proprio perché consente di condividere informazioni sensibili solo con alcuni partner selezionati, senza rivelare informazioni riservate a potenziali concorrenti. Il loro utilizzo, quindi, è principalmente nel settore imprenditoriale. Un esempio di blockchain permissioned è il progetto Hyperledger promosso e finanziato dalla Linux Foundation.

[107] *Ibidem*
[108] https://101blockchains.com/permissioned-blockchain/

3.2.1. Hyperledger

Hyperledger è un progetto della Linux Foundation nato nel 2015. L'obiettivo è quello di creare una *cross industry* nel mondo delle blockchain. È un progetto a cui partecipano una pluralità di soggetti, tra cui imprese, leader nel mondo bancario e della finanza, catene di montaggio e molti altri ancora[109]. L'obiettivo non consta nel creare una nuova blockchain, ma nel collaborare e dare vita ad una community. Si può, quindi, affermare come Hyperledger sia una specie di grande contenitore in cui sono inseriti diversi progetti. Questa idea di creare una comunità in cui condividere idee e innovazioni a livello tecnologico nasce quando più imprese interessate al mondo blockchain hanno compreso come si possa ottenere di più, in termini di sviluppo e redditività, collaborando[110]. È curiosa la scelta di rendere tutti i progetti finanziati, tra cui il più celebre Hyperledger Fabric, open source, ovverosia il codice sorgente è aperto al pubblico permettendo a chiunque di scaricarlo, modificarlo e personalizzarlo a piacere. È una strategia di marketing, in quanto in questo modo si riesce ad ottenere un numero maggiore di partners e di soggetti intesi ad investire in questo progetto e quindi di ridurre i rischi ed essere maggiormente competitivi. Inoltre l'essere open source, come scritto del white paper, permette di garantire la interoperabilità tra sistemi diversi. L'interoperabilità è fondamentale in quanto, ad oggi, sono presenti una pluralità di programmi, spesso scritti con linguaggi diversi, che devono essere in grado di comunicare tra loro in un contesto business to business. Le caratteristiche principali di Hyperledger sono: (i) la modulabilità, ossia personalizzazione; (ii) la presenza di un elevato livello di sicurezza; (iii) l'interoperabilità; (iv) l'assenza di criptovalute ed infine (v) l'essere completo grazie all'utilizzo dell'APIs che permette di avere un'interfaccia user friendly[111]. Le caratteristiche più rilevanti sono, però, l'essere altamente modulare, l'interoperabilità e l'essere priva di criptovalute. L'essere modulare implica la possibilità per i programmatori di sperimentare con diverse tipologie di componenti e di cambiare alcuni specifici elementi senza inficiare sull'intero sistema[112]. Hyperledger permette, quindi, la personalizzazione delle singole componenti. L'interoperabilità è un traguardo importante da raggiungere perché permette a diverse tipologie di blockchain di interagire e scambiare dati. Inoltre grazie all'interoperabilità non vi è più la necessità di dover scambiare informazioni con la stessa tipologia di blockchain e questo è un fattore che, in futuro, permetterà una maggior diffusione delle blockchain e delle tecnologie a registro distribuito[113]. La caratteristica che rende Hyperledger un sistema diverso da tutti gli altri è l'assenza di criptovalute, ossia l'essere *cryptocurrency-agnostic.* È

[109] Tratto da https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/HL_Whitepaper_IntroductiontoHyperledger.pdf
[110] *Ibidem*
[111] *Ibidem*
[112] *Ibidem*
[113] *Ibidem*

una scelta coerente con quanto si sostiene nel white paper, in quanto Hyperledger ha come obiettivo quello di creare software favoriscano l'utilizzazione della tecnologia blockchain nelle imprese e non la gestione o creazione di nuove monete virtuali.

3.2.2.1. Hyperledger Fabric

Hyperledger, si è detto, può essere considerato come un grande contenitore all'interno del quale sono inseriti una varietà di strumenti e di progetti. Tra questi il più famoso e che rientra nella categoria di blockchain *permissioned* è Hyperledger Fabric. Hyperledger Fabric è una piattaforma disegnata per la creazione di soluzioni a registro distribuito, modulari garantendo un elevato livello di confidenzialità, flessibilità, resilienza e scalabilità[114]. È una piattaforma il cui funzionamento si basa sul modello esegui – ordina – valida, ossia *l'execute – order – validate*[115]. All'interno di questa struttura si distinguono tre nodi[116]: (i) i nodi che sono responsabili per le transazioni autorizzate, ossia gli *endorsers;* (ii) i nodi che distribuiscono i blocchi, ovvero gli *orderers* ed infine (iii) dopo la distribuzione dei blocchi, essi vengono confermati dai *commiter nodes.* Il protocollo che viene utilizzato da Hyperledger Fabric suddivide la procedura di validazione del blocco in tre fasi: esecuzione, organizzazione dell'ordine delle transazione ed infine validazione della transazione[117]. Il procedimento può essere così riassunto. Nella prima fase di esecuzione, un cliente invia una transazione firmata crittograficamente a uno o più endorsers affinché si dia avvio alla procedura. Successivamente viene stabilito l'ordine delle transazioni per passare all'ultima fase, ovvero la validazione. In questa fase i nodi controllano se le transazioni soddisfano i requisiti previsti dall'*endorsement*. I nodi *endorses*, infatti, fungono da autorità che controlla la rete blockchain permettendo l'accesso solo ad alcuni soggetti, individuando chi può scrivere e leggere dati e chi li può configurare[118]. Una volta effettuata questa verifica, i nodi aggiungono il blocco al registro. È un sistema piuttosto semplice e veloce nel funzionamento. Veloce anche nel senso che possono essere creati appositi canali separati dal resto della catena che eseguono ulteriori transazioni, facendo sì che si crei una sub-rete blockchain.[119] Un ulteriore caratteristica di Hyperledger Fabric che distingue questa blockchain da tutte le altre è l'utilizzo di smart contract, che nell'ambito vengono chiamati *chaincode,* i quali utilizzano un linguaggio di programmazione come Java, quindi linguaggi di programmazione di carattere generale e non del dominio stesso, come accade, invece, in Ethereum[120]. Questo è un enorme vantaggio in quanto permette a chiunque sia in grado di

[114] *Ibidem*
[115] Guggenberger, Sedlmeir, Fridgen, & Luckow, 2022
[116] https://medium.com/geekculture/introduction-to-hyperledger-fabric-1ce0a1d67494
[117] Si veda nota n.115
[118] Si veda nota n.116
[119] *Ibidem.*
[120] Brotsis, Kolokotronis, Limniotis, Bendiab, & Shiaeles, 2020

programmare con Java o con altri linguaggi di sfruttare tale servizio. È un aspetto che non deve essere sottovalutato trovandosi in un contesto business to business è lapalissiano come le imprese utilizzino linguaggi come Java Script, C++ o Phyton. Questo permette di sfruttare Hyperledger Fabric senza dover investire sulla formazione del personale con conseguente risparmio in termini economici e di tempo. Si osserva, poi, i protocolli di consenso che vengono utilizzati non sono del tipo *proof* come in Bitcoin o in Ethereum. I protocolli che vengono maggiormente utilizzati sono Apache Kafka e Raft[121]. Apache Kafka può essere descritto come un servizio di messagistica che viene utilizzato per il trasferimento di dati. Il modello che viene seguito è quello del leader – follower: vi è chi è in una posizione di guida e chi è in una posizione di mero esecutore degli ordini del leader. Anche Raft segue il modello leader – follower. Per garantire una maggiore coesione tra i nodi, il protocollo è separato in tre fasi: l'elezione del leader, la replica del registro e la sicurezza. I nodi sono suddivisi gerarchicamente per cui ogni nodo può essere un leader, un candidato o un follower. La sincronizzazione dei dati viene garantita tramite l'invio di impulsi, in gergo battiti cardiaci, ai follower. In questo modo se uno dei nodi della rete dovesse sospettare che il leader si sia bloccato, vi è la possibilità di eleggere un nuovo leader e garantire la sincronizzazione[122]. Questi sono protocolli che non richiedono alcun tipo di prova né alcun tipo di sfruttamento di elevati poteri di calcolo per la risoluzione di complessi problemi matematici a differenza dei protocolli di consenso maggiormente diffusi.

3.3. Blockchain consortium

Consorzio deriva dal latino consortium, ossia *partecipazione alla stessa sorte, società, comunanza di beni*[123]. L'etimologia del lemma dà un indizio sulla natura della terza tipologia di blockchain presente, ossia la blockchain consortium. Spesso viene confusa con la tipologia *permissioned*, in quanto condivide alcuni tratti ma si differenzia per altri. Le blockchain consortium, conosciute anche come *federated,* prevendono un insieme di organizzazioni che si uniscono per far fronte ad un bacino di esigenze comuni unendo elementi della blockchain pubblica e privata[124]. È, quindi, una forma ibrida. Per poter entrare a far parte della rete è necessario ottenere una autorizzazione, ma a differenza della blockchain *permissioned* nella quale tale processo viene effettuato da una sola entità facendo sì che ci sia una centralizzazione del sistema, nella tipologia consortium, invece, il processo di selezione viene effettuato da una pluralità di enti garantendo, quindi, la decentralizzazione. A differenza delle altre due

[121] *Ibidem*
[122] *Ibidem*
[123] Enciclopedia Treccani, voce consorzio.
[124] https://101blockchains.com/federated-blockchain/

tipologie di blockchain, i consorzi per quanto riguarda la procedura di creazione e validazione di un nuovo blocco non prevedono l'utilizzo di un algoritmo di consenso come il Proof – of – Stake o il Proof – of – Work o variazioni di essi. Affinché un blocco venga aggiunto alla catena si utilizza un sistema di votazione il cui quorum è predeterminato dagli enti partecipanti al consorzio[125]. Il fatto di utilizzare dei sistemi di votazione per raggiungere il consenso implica un notevole risparmio in termini energetici, in quanto i nodi non devono effettuare alcun tipo di procedimento di *mining*, ergo tale tipologia di blockchain ha un impatto ambientale notevolmente ridotto rispetto alle reti che utilizzano i tradizionali protocolli di consenso. Il far parte di una blockchain consortium pone una serie di vantaggi sia dal punto di vista della sicurezza sia dal punto di vista dell'efficienza del sistema. Per quanto riguarda la sicurezza, in questa tipologia di blockchain è pressoché nullo il rischio di essere sottoposti ad attacco, in quanto le autorità di controllo non permettono l'ingresso a chiunque e soprattutto non vi è alcun rischio connesso alla attività criminale[126]. Essendo presenti pochi nodi all'interno del network questo implica una maggior velocità nelle transazioni e una riduzione dei costi per effettuare tali operazioni. Questo implica anche il fatto che nelle blockchain consortium viene risolto il problema della scalabilità, ossia è in grado di sopportare un aumento del carico di lavoro senza compromettere l'efficienza del sistema. Questa tipologia di blockchain è sotto i riflettori soprattutto nel settore imprenditoriale e più nello specifico nel settore del luxury.

3.3.1. Aura blockchain

Aura blockchain è un esempio concreto dell'utilizzazione delle blockchain consortium e dello sfruttamento delle sue potenzialità in un settore molto redditizio quanto delicato, ovvero quello del lusso. Nel 2021 LVMH, Mercedes – Benz, OTB, Prada Group e Richemont si sono uniti e hanno fondato Aura, una organizzazione non profit. Sembra un paradosso il fatto che brand di lusso in competizione tra loro si siano alleati per dare vita a tale progetto, ma come descritto nel sito ufficiale, la *vision* è nel credere che una collaborazione possa coesistere assieme alla competizione per raggiungere un bene superiore[127]. L'obiettivo è quello di mettere al centro il cliente offrendogli trasparenza e tracciabilità del prodotto[128]. È questo l'obiettivo che ha spinto i più grandi marchi del lusso a dare vita ad un consorzio per rendere la *customer experience* un'esperienza a tutto tondo. Il cliente tramite l'impiego di questa blockchain ha la possibilità di avere accesso diretto alla storia del prodotto partendo dal reperimento dei materiali e controllando la loro origine per poi essere coinvolto

[125] Si veda nota n.124
[126] *Ibidem*
[127] Aura consortium – about, per ulteriori informazioni si veda https://auraconsortium.com/about
[128] *Ibidem*

nel ciclo di produzione e di distribuzione nei negozi fisici e online. Il tutto avviene tramite un ID digitale unico per ogni tipo di prodotto. Questo ID è sottoforma di codice QR ed è contenuto nel DPP, ossia nel *Digital Product Passport*[129]. Il QR code è presente sull'etichetta della merce che scannerizzato con lo smartphone permette di accedere a tutte le informazioni che la riguardano. Il passaporto digitale del prodotto consente di garantirne l'autenticità, il che è molto importante per il mondo luxury in quanto è particolarmente diffuso il fenomeno della contraffazione. Il fatto che tutte le informazioni che riguardano la merce siano inserite all'interno della blockchain permette di sfruttare tutte le potenzialità offerte da questa tecnologia, soprattutto l'immutabilità. Ad esempio, il brand di lusso X può indicare che la sua borsa ha determinate caratteristiche come la fibbia elaborata in un certo modo o l'apposizione del logo in una certa direzione. Una volta che queste informazioni sono inserite all'interno della blockchain, esse non possono essere più modificate e questo rende più facile verificare se il prodotto sia autentico o contraffatto da parte delle autorità competenti. Con il *Digital Product Passport* viene garantita anche la tracciabilità del prodotto e l'interazione con il cliente, fattore cruciale in questo settore. L'avere a disposizione in qualsiasi momento un professionista che accompagni il cliente nella scelta dell'articolo o nell'assistenza è l'elemento che distingue i marchi di lusso da tutti gli altri brand. Aura blockchain, oltre a fornire il servizio di passaporto digitale prevede anche i *Digital Collectibiles*[130]*,* ossia viene ridefinito il concetto stesso di loyalty del cliente. Tramite la collezione di NFT a seguito dell'acquisto del bene, il marchio mostra un segno di apprezzamento nei confronti del cliente offrendogli, ad esempio, premi fedeltà, vantaggi per le riparazioni e servizi post-vendita. Aura blockchain è solo uno dei tanti esempi di applicazione concreta delle blockchain consortium che prevedono una serie di vantaggi non solo per l'audience, ma anche per le società che vi partecipano, per esempio esse beneficiano di una relazione tête-à-tête con la clientela. Vi è, poi, uno sguardo verso il futuro con l'obiettivo di utilizzare il 100% di energia rinnovabile e la collaborazione con altri marchi di lusso per consentire lo sviluppo di tale tecnologia[131].

[129] *Ibidem*
[130] *Ibidem*
[131] Aura consortium - customer journey, per ulteriori informazioni si veda https://auraconsortium.com/customer-journey

4. Esempi di utilizzazione della tecnologia blockchain

È evidente come la tecnologia blockchain, grazie alle sue caratteristiche e così come descritta nel suo funzionamento, possa essere applicata in diversi settori. Tra questi si considerano le cc.dd. *smart cities* e il settore sanitario. Lo studio è stato circoscritto a questi ambiti, in primis, per una esigenza espositiva. Sarebbe sato eccessivo considerare ogni possibile applicazione della blockchain rendendo, conseguentemente, la trattazione tediosa e poco interessante. Vi è, poi, una ragione di carattere sociologico. Nella vita quotidiana si è a costante contatto con la tecnologia, dunque, emerge la necessità di comprenderne il funzionamento per poter valutare i benefici che essa apporta e sollevare eventuali dubbi derivanti dalla sua utilizzazione. Le città in cui si vive e la sanità sono solo alcuni degli aspetti della vita quotidiana in cui può inserirsi la blockchain per apportare delle migliorie, o, quanto meno cercare di risolvere alcune problematicità presenti in questi ambiti. L'obiettivo, dunque, è quello di cercare di sviluppare un pensiero critico circa l'utilità di tale tecnologia che si può costruire partendo proprio dallo studio della blockchain e delle sue possibili applicazioni. La terza ragione, infine, che motiva l'esame dell'impiego della blockchain in questi settori è la semplice curiosità alimentata dall'esigenza di comprendere il funzionamento di tale tecnologia in ambiti diversi da quello per cui è stata originariamente progettata, ossia il settore finanziario. Si può affermare con un certo grado di certezza che la ricerca in questo campo si sia concentrata principalmente sulla finanza, trascurando le ulteriori possibilità di applicazione e ignorando, di conseguenza, i vantaggi che essa può apportare se adeguatamente implementata fornendo, dunque, una soluzione alle sfide che la vita quotidiana pone.

4.1. Le smart cities

Non è semplice descrivere che cosa sia una città intelligente, in quanto non è presente una definizione universalmente accettata. La città intelligente, infatti, risulta essere un concetto piuttosto ampio che racchiude diversi aspetti della vita cittadina che vanno dal trasporto pubblico, alla gestione delle risorse energetiche ed idriche all'*e-government*[132]. Dai vari tentativi di definire tale fenomeno è emerso in letteratura un elemento in comune, ossia l'utilizzazione delle ICT in diversi settori per migliorare la qualità della vita dei cittadini e sfruttare in maniera più intelligente le risorse energetiche a disposizione ponendo uno sguardo allo sviluppo di città più attente al tema della sostenibilità e del cambiamento climatico.

[132] Per e-governement si intende *"l'uso delle tecnologie dell'informazione e della comunicazione nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostengo alle politiche pubbliche".* Tratto da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52003DC0567

Solo in tempi relativamente recenti si è iniziato a parlare di *smart city*. Nel 2008 nel pieno della crisi economico – finanziaria IBM propose il concetto di città intelligente. Secondo la definizione fornita dal colosso informatico, per *smart city* si intende l'applicazione dell'*Internet of Things*[133]che collega risorse pubbliche come reti elettriche, autostrade e sistemi di fornitura d'acqua tramite diverse tipologie di sensori diffusi per il territorio cittadino[134]. Nella *smart city* siano coinvolti diversi fattori, ossia quello umano, urbanistico, ecologico e, ovviamente, tecnologico. Il fattore umano deve essere associato a quello urbanistico, in quanto l'obiettivo è quello di creare città a misura d'uomo, ossia città che soddisfino le esigenze dei residenti, quali la riduzione dell'inquinamento atmosferico, la creazione di spazi verdi e dal punto di vista dell'amministrazione, l'erogazione di servizi online. Oltre a soddisfare le esigenze dei residenti più attenti al proprio benessere e consapevoli del fatto che le città sono sempre più di cemento, vi è da considerare anche il fattore ecologico e tecnologico. Il fattore ecologico è strettamente correlato con i primi due, in quanto l'obiettivo che si vuole raggiungere è quello sviluppare città che siano più attente alla questione della sostenibilità e dell'inquinamento tramite l'utilizzazione delle tecnologie a disposizione che consentono di migliorare l'approvvigionamento delle risorse energetiche e la loro gestione andando a ridurre i costi sia per gli utenti che per l'amministrazione cittadina. Il fattore tecnologico, però, è l'elemento portante per una città intelligente. Senza la tecnologia non è possibile realizzare gli obiettivi che la *smart city* intende perseguire. Inoltre, se non fosse presente tale fattore la città non potrebbe definirsi *smart.* L'architettura alla base di ogni *smart city* comprende tre elementi, ossia (i) un database che raccoglie e conserva tutte le informazioni che riguardano la città , (ii) sistemi di controllo intelligenti che organizzano i dati raccolti e (iii) la presenza di sistemi IT, principalmente sensori diffusi in tutto il territorio cittadino, che raccolgono informazioni in tempo reale circa, ad esempio, le risorse disponibili o la congestione del traffico consentendone un monitoraggio costante[135]. La città intelligente, quindi, può essere considerata sotto due profili. Il primo aspetto pone attenzione al capitale umano in continuo aumento a seguito della crescita demografica, dunque, sorge la necessità per il residente di vivere in luogo che soddisfi al meglio le proprie esigenze. Ad oggi, infatti, c'è una maggior consapevolezza dell'importanza dell'ambiente in cui si vive e di come esso influisca sul benessere psicofisico, per cui tale aspetto risulta essere un fattore cruciale per migliorare o peggiorare la qualità della vita. Il secondo profilo, invece, riguarda l'unione tra città e tecnologia quale elemento necessario per migliorare la qualità della vita dei residenti. L'essenza, dunque, della *smart city* risiederebbe non tanto nelle

[133] Termine coniato nel 1999 da Kevin Ashton per descrivere un sistema nel quale Internet è connesso al mondo fisico attraverso sensori ubiqui. Tratto da https://www.historyofinformation.com/detail.php?id=3411
[134] Makani , Pittala, Alsayed, Aloqaily , & Jararweh, 2022
[135] Sun, Yan, & K. Zhang , 2016

infrastrutture e nelle tecnologie all'avanguardia utilizzate, ma nell'individuare i bisogni dei cittadini e trovare delle soluzioni per poterli soddisfare utilizzando la tecnologia a disposizione[136]. Descritta la panoramica sul perché si parla di città intelligenti, è possibile, dunque, trattare alcuni casi. La città di Tempe in Arizona è un esempio di *smart city* che utilizza la tecnologia blockchain nel settore idrico per lo scambio di diritti inerenti a questo bene prezioso. L'idea di fondo è quella di impiegare la blockchain per far fronte all'aumento della domanda e la riduzione dell'offerta e alla gestione delle risorse idriche, soprattutto in zone ad elevato rischio di siccità come l'Arizona. L'utilizzazione della blockchain in questo ambito consente di controllare il mercato idrico e lo scambio di *trading rights* tale da evitare che vi sia speculazione su questo bene prezioso, a beneficio di tutti i residenti. I vantaggi[137] che derivano dall'utilizzazione della blockchain in questo contesto sono molteplici tra cui (i) una riduzione dell'iniquità permettendo ai sistemi idrici con un surplus di acqua di trasferire l'eccesso a sistemi che sono in deficit; (ii) uno sviluppo di nuove forme di reddito incoraggiando le reti idriche locali a sfruttare diverse fonti di approvvigionamento, come l'acqua piovana andando, di conseguenza, a diversificare le risorse per poter far fronte ad eventuali crisi idriche ed infine (iii) la creazione di incentivi per le reti idriche allo scopo di riciclare l'acqua di scarto, affinché vi sia vi sia un riciclo continuo e un risparmio di risorse.

Il progetto CitySense è un ulteriore esempio di utilizzazione della blockchain nelle grandi città. CitySense è un sensore che viene utilizzato per misurare diversi parametri, quali la concentrazione di microparticelle nell'aria, il rumore, la temperatura, l'umidità etc. per valutare il livello di inquinamento atmosferico[138]. È, quindi, un sensore che nella sua utilizzazione risulta essere versatile, in quanto viene utilizzato anche in altre aree, come l'illuminazione stradale. Tale sensore, infatti, rileva la presenza di automobili, pedoni e ciclisti e aumenta l'intensità della luce in base al soggetto rilevato comportando ad un risparmio in termini di emissione di CO_2 e dei costi energetici e di manutenzione dell'illuminazione[139]. Al di là della versatilità d'utilizzo, CitySense si basa sulla tecnologia blockchain per indagare alcuni aspetti dell'*urban setting* ed elaborare le informazioni ricevute utilizzando Ethereum per registrare i dati provenienti dai sensori presentando un'architettura a strati composta dal *physical layer,* dal *network layer*, dal *database layer* ed infine dall'*application layer*[140].

---

[136] Treiblmaier , Rejeb , & Strebinger, 2020

[137] S. Alnahari & T. Ariaratnam, 2022

[138] Ibba , Pinna, Seu, & Pani, 2017

[139] Tratto da https://www.tiot.it/smart-city/illuminazione-stradale-solo-dove-e-quando-serve/

[140] Il *physical layer*, prevede l'utilizzazione di sensori con la funzione di raccogliere dati e trasmetterli nella fase successiva di elaborazione. Il *communication layer* sfrutta diversi protocolli di comunicazione come il 3G, il 4G e il Wi-fi. I dati inviati dai sensori sono del tutto anonimi e vengono aggiunti nella blockchain al fine di essere inseriti in blocchi o per essere impiegati per la conclusione di smart contract nella piattaforma Ethereum, la più utilizzata in tale settore. Il *database layer*, invece, funge da archivio dei dati raccolti tramite l'utilizzazione di un registro distribuito, quale la blockchain. Si veda M. Ghazal, et al., 2022

La blockchain oltre ad essere utilizzata per uno specifico fine, come nel caso di CitySense, può essere applicata in ogni aspetto della vita cittadina e Smart Dubai ne è un esempio. La città di Dubai negli Emirati Arabi Uniti si è posta come obiettivo di essere la prima città al mondo governata totalmente dalla blockchain entro il 2020[141] . La necessità di utilizzare tale tecnologia su larga scala trae origine dallo sviluppo di Dubai che in poche decadi è passata da essere un piccolo centro cittadino nel deserto ad una metropoli con più di tre milioni di abitanti. Il suo rapido sviluppo in diversi settori dell'economia ha fatto sì che vi fosse l'esigenza di riqualificare tale settore per poter assicurare efficienza e velocità nelle operazioni economiche. Dubai, dunque, è una città smart a tutto tondo e ciò si riconosce nell'utilizzazione da parte del *Dubai Economic Department*[142] della blockchain per lo sviluppo di piani economici e per attirare nuovi *businesses* che favoriscano la crescita della città. L'adozione della blockchain, però, non è stata immediata. In origine il DED utilizzava un sito web nel quale vi era un elenco di tutte le attività commerciali. Tale sito web fungeva, dunque, solo da mero elenco. Successivamente, il dipartimento cominciò ad offrire servizi online per la concessione di licenze a fini commerciali tramite la piattaforma Dubai.ae. Nel 2017 vi è il punto di svolta con l'adozione della blockchain riservata al settore imprenditoriale e l'anno successivo venne creato l'*Unified Business Registry* come piattaforma di condivisione di informazioni e registrazione dei dati. Gli utenti accedono a tale registro tramite il portale MyId potendo, quindi, utilizzare ogni servizio governativo presente nella piattaforma. Tale piattaforma si basa sulla blockchain e in particolare viene utilizzata la blockchain appartenente alla categoria consortium. L'autorità di controllo è il DED, il quale individua chi possa fare parte della rete, quali dati possono essere letti dalle altre autorità governative e quali informazioni possono essere visibili agli utenti della rete. La rete blockchain consente al DED di essere connesso ad altre autorità governative, dunque, tutte le operazioni vengono registrate presso un'unica rete blockchain con conseguenti vantaggi. In primis, vi è una riduzione dei costi di operazione. Il modello di riferimento è il *pay as you go,* per cui l'utente paga solo il servizio utilizzato. Inoltre, l'utilizzazione di tale tecnologia permette di aumentare il livello di fiducia tra gli operatori commerciali in assenza di parti terze che fungono da intermediari e in presenza di procedure più semplici e veloci tra diverse autorità governative interconnesse tra loro[143]. Dubai, però, si pone un ulteriore obiettivo, ossia di diventare la capitale mondiale della blockchain tramite una serie di iniziative, come la *Smart Dubai Global Blockchain Challenge* ossia una gara che si tiene annualmente con lo scopo di selezionare i migliori progetti al mondo in tale settore ed investendo, inoltre,

[141] Tratto da https://www.digitaldubai.ae/initiatives/blockchain
[142] Da ora in poi DED
[143] Khan , Shael , Majdalawieh , Nizamuddin, & Nicho, 2022

sull'istruzione coinvolgendo scuole e università[144] in diversi progetti che riguardano tale tecnologia. Si è compreso, infatti, che per diventare il leader mondiale in questo settore si deve partire dal basso con un'educazione digitale che coinvolga qualsiasi fascia d'età per formare la generazione del futuro che sia familiare con tale tecnologia per poterla implementare e sfruttare al meglio.

Le *smart cities,* dunque, danno prova di essere un terreno fertile per l'applicazione della blockchain grazie alla quale è possibile affrontare le varie sfide che l'urbanizzazione, l'inquinamento e il benessere dei residenti pongono. I benefici che tale tecnologia apporta in questo contesto non sono ancora del tutto esplorati per una insufficienza di informazioni a riguardo. Si può, quindi, affermare come questo sia un settore ancora poco studiato e in continua crescita. Sicuramente la città di Dubai risulta un paradigma a cui attingere per lo sviluppo di nuove *smart cities* e per comprendere le potenzialità della blockchain in tale ambito.

4.2. Il settore sanitario

Con il passare del tempo si è consolidato il legame tra il settore sanitario e quello tecnologico. Questa *liaison* non riguarda solo i progressi della scienza nel campo diagnostico e della ricerca, ma anche nell'utilizzazione di nuove tecnologie, quali la blockchain, per far fronte ad alcune sfide come la condivisione dei dati dei pazienti, la fornitura dei farmaci e il loro tracciamento. L'utilizzo della tecnologia in questo ambito è relativamente recente. Negli anni '70 del secolo scorso[145] i referti e le cartelle cliniche erano su supporto cartaceo. Tale era la tecnologia presente all'epoca, la quale comportava alcuni svantaggi come la registrazione dei dati dei pazienti piuttosto lunga e laboriosa dovendo essere eseguita manualmente, oltre al rischio che le cartelle cliniche venissero perse per fattori esterni quali eventi naturali o per mero errore umano. Tra il 1991 e il 2005 salute e tecnologia iniziano ad interfacciarsi l'una all'altra. In questo periodo si registrano notevoli progressi con l'introduzione del monitoraggio digitale e di sistemi di *imaging*[146] sempre più accurati per poter tracciare al meglio la salute dei pazienti[147] e fornire, conseguentemente, immagini più nitide che permettessero diagnosi più accurate. È curioso osservare come questo legame si formi in concomitanza della nascita dei primi social network. I sistemi di *healthcare* comprendono le potenzialità dei social creando le prime communities online per la condivisione di informazioni inerenti alla salute. Ad esempio, una delle communities più famose in Italia è *medicitalia.it,* piattaforma web gratuita, fondata nel 2000, che

[144] Bishr, 2019
[145] Tanwar , Parekh , & Evans, 2019
[146] Per sistemi di *imaging* si intendono radiografia, ecografia, TAC e risonanza magnetica.
[147] Si veda nota n.145

fornisce consulti medici e divulgazione medico – scientifica[148]. Con il cc.dd. Web 3.0[149] viene sviluppato il concetto di *e-health,* ossia di sanità digitale. In questa fase non è più presente l'analogico, anche se non è del tutto scomparso, in quanto le cartelle cliniche vengono digitalizzate creando, così, i fascicoli elettronici. Lo sviluppo tecnologico si ravvisa anche nella cc.dd. *mobile health*, ossia l'utilizzazione delle ICT a supporto della salute e dei campi collegati ad essa[150]. Con la *mobile health,* dunque, compaiono i primi dispostivi indossabili, come gli smartwatch per il tracciamento e la misurazione di alcuni parametri vitali, quali il battito cardiaco o i passi. La *mobile health* include anche applicazioni che tengono traccia dei dati ottenuti da tali dispositivi. Le applicazioni possono essere installate di default*,* come "Salute" presente in tutti i dispositivi Apple, o possono essere scaricate dai rispettivi App Store e Play Store. Nel Web 3.0, inoltre, emerge un legame sempre più forte tra digitalizzazione e settore sanitario con l'archiviazione online dei dati dei pazienti rendendo la loro condivisione più efficiente[151]. L'*e-health,* dunque, è il frutto dell'unione tra salute e tecnologia. Non è presente una definizione univoca, ma agli inizi degli anni 2000 Eysenbach cercò di inquadrare il concetto in questi termini: *"E-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology"*[152]. Da questa definizione emergono gli elementi chiave della salute digitale, ossia l'utilizzazione delle ICT nel settore sanitario che ha come obiettivo migliorare l'assistenza sanitaria non solo a livello locale, ma anche globale. Il risultato è un intreccio tra l'informatica medica, la sanità pubblica e l'imprenditoria per una più adeguata ed efficiente fornitura dei servizi sanitari. La definizione così fornita è ampia, ma tale ampiezza non deve essere considerata in maniera negativa, in quanto l'intento è quello di abbracciare ogni aspetto che la sanità digitale va a toccare. Nell'*e-health* oltre all'utilizzazione delle tecnologie dell'informazione e della comunicazione a supporto del sistema sanitario, è pensabile anche l'utilizzazione delle blockchain, le quali fornirebbero un supporto in questo settore per rendere l'intero sistema più efficiente. I problemi che si riscontrano maggiormente sono (i) la condivisione dei dati dei pazienti tra diverse strutture ospedaliere che si concretizza nella mancanza di interoperabilità, (ii) la gestione delle cartelle cliniche ed infine (iii) il tracciamento dei farmaci e la lotta alla criminalità contro la contraffazione e il contrabbando.

[148] Tratto da https://www.medicitalia.it/chi-siamo/
[149] Il Web 3.0. è la nuova generazione di Internet che sfrutta il machine learning, l'intelligenza artificiale e la blockchain.
[150] World Health Organization, 2018
[151] Tanwar , Parekh , & Evans, 2019
[152] Eysenbach, 2001

L'obiettivo è quello di utilizzare al meglio le caratteristiche della blockchain, tra cui l'immutabilità, la decentralizzazione e l'accesso controllato per superare questi ostacoli. Una delle sfide più grandi che tale ambiente pone è la gestione e l'archiviazione dei dati. Ogni giorno vengono create innumerevoli quantità di dati che vengono conservate in sistemi centralizzati, il che è un rischio, in quanto in caso di malfunzionamento del server l'intero apparato cessa di funzionare. Ecco, dunque, come la blockchain può essere applicata per porre rimedio a questo problema usufruendo una delle sue caratteristiche principali, ossia la decentralizzazione. Se i dati dei pazienti vengono archiviati su una rete decentralizzata in cui ogni nodo detiene una copia, nel caso in cui uno o più nodi non dovessero funzionare, i dati sono comunque recuperabili in quanto presenti in tutti gli altri *peers* della rete. I dati sanitari, inoltre, è pacifico che possano essere inseriti nella rete, in quanto, uno dei punti di forza della blockchain consiste nella sua versatilità: nella rete è possibile effettuare qualsiasi tipo di transazione e registrare qualsiasi tipologia di dato. Impiegando tale tecnologia i pazienti, inoltre, sono in grado di controllare i propri dati decidendo chi possa accedervi, quali mostrare e per quanto tempo[153]. In questo modo, dunque, al paziente viene fornita l'opportunità di gestire al meglio le informazioni che lo riguardano e comprendere come vengano utilizzate e per quali finalità. Si pone, in questo caso, un problema riguardante la prestazione del consenso[154] . Per poter accedere alla cartella clinica, infatti, è necessario che il diretto interessato abbia fornito il proprio consenso all'operatore che ne faccia richiesta. Nella maggior parte dei casi in queste occasioni la tipologia di blockchain che viene utilizzata appartiene alla categoria *permissioned* per cui non vi è un accesso garantito a tutti, ma solo a soggetti che vengono approvati da un'autorità centrale in quanto soddisfacenti dei requisiti previsti dalla rete stessa. In questa circostanza, dunque, non si prende in considerazione un'ipotetica situazione di emergenza nella quale la persona interessata si trovi in una condizione di incapacità di intendere e di volere non essendo, quindi, in grado di prestare il consenso. Per ovviare a questo problema si potrebbe utilizzare la tecnologia blockchain. Una soluzione viene proposta da Medicalchain, piattaforma decentralizzata utilizzata per lo scambio di dati sanitari. Grazie a questa piattaforma l'utente può decidere quali dati fornire in caso di emergenza, ad esempio gli elementi identificativi[155]. Medicalchain, inoltre, prevede l'utilizzo di un braccialetto, il cc.dd. *emergency bracelet,* sul quale è presente un codice QR che, una volta scannerizzato, dà libero accesso ai dati dell'utente[156]. Medicalchain è una delle tante piattaforme presenti nel settore sanitario che permette di condividere i

[153] Medicalchain, 2018

[154] Ai sensi dell'art.4 del Reg. n. 679/2016 per "consenso dell'interessato" si intende "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

[155] Come il nome, il cognome, l'età, il gruppo sanguigno, allergie, patologie etc.

[156] Medicalchain, 2018

dati in totale sicurezza, superando l'ostacolo dell'interoperabilità, ossia il problema attinente alla condivisione dei dati tra diverse fonti, quali strutture ospedaliere e operatori sanitari. Medicalchain utilizza Hyperledger Fabric, appartenente alla categoria della blockchain *permissioned*, per gestire l'accesso alle cartelle cliniche ed Ethereum, la quale racchiude tutte le funzionalità della piattaforma. Per assicurare la protezione dei dati inseriti viene utilizzata la crittografia a chiave simmetrica, dunque, ogni volta che un soggetto ottiene il permesso di accedere ai dati dell'utente, il dato viene decriptato con la chiave privata dell'interessato e la chiave simmetrica viene crittografata con la chiave pubblica dell'utente a cui viene dato accesso[157]. Una volta che viene garantito l'accesso ai dati viene avviato un procedimento in più passaggi. In primis i dati di cui si richiede la visione vengono sottoposti a hashing. Una volta ottenuta la stringa di hash corrispondente vengono effettuate due operazioni, ossia (i) i dati vengono crittografati e memorizzati e (ii) la stringa di hash viene inserita nel registro. A questo punto, l'hash del registro e l'hash dei dati memorizzati nell'archivio vengono confrontati. Se le stringhe coincidono, allora i dati richiesti vengono inviati al richiedente, altrimenti l'operazione si conclude con una segnalazione se i dati risultano essere compromessi. Medicalchain, inoltre, è fornito di propri token, ossia i MTN che permettono di accedere ai servizi forniti dalla piattaforma, quali consultazioni in via telematica, la cc.dd. telemedicina, condivisione dei dati sanitari per fini di ricerca e per fini assicurativi. È interessante osservare come tale condivisione avvenga per diverse finalità e come i dati, sostanzialmente, diventino una merce di scambio, una sorta di *do ut des.* L'utente fornisce i propri dati e in cambio riceve MedTokens da utilizzare sulla piattaforma o degli sconti, in termini di premi assicurativi. In conclusione, Medicalchain risulta essere una piattaforma multifunzione che promette agli utenti di avere un controllo maggiore sui dati che li riguardando e un elevato grado di sicurezza, in quanto la tipologia di blockchain utilizzata appartiene alla categoria *permissioned.* Un'ulteriore sfida che è presente nel settore sanitario è la gestione delle cartelle cliniche. Sfida che, come antagonista, ha il sistema ideato da Azaria, Ekblaw, Vieria e Lippman nel 2016, ossia MedRec. MedRec è un servizio creato per la gestione delle cartelle cliniche elettroniche permettendone la condivisione tra diversi operatori del settore grazie all'utilizzo della blockchain. Il problema che MedRec intende risolvere è la frammentazione dei dati presenti all'interno delle cartelle cliniche, in quanto è evidente come vi sia una produzione di dati sanitari afferenti a diverse fonti. Non sono, infatti, presenti solo le informazioni riguardanti la storia clinica del paziente presso il medico curante, ma anche presso i medici specializzati. L'obiettivo, dunque, è quello di racchiudere tutta la storia clinica in un unico documento in modo da avere un quadro completo che ne faciliti la condivisione e permetta di effettuare delle diagnosi più accurate ponendo attenzione, anche, alla riservatezza dei pazienti. Tale sistema si basa

[157] *Ibidem*

sull'utilizzo degli smart contract presenti su Ethereum associando la cartella clinica al consenso fornito dal diretto interessato per il recupero dei dati e l'esecuzione degli smart contract su database esterni. MedRec si basa su tre contratti: il *Registrar Contract (RC),* il *Patient – Provider Relantionship Contract (PPR)* e il *Summary Contract (SC)*[158]. Il *Registrar Contract* è un contratto di carattere generale che traccia le stringhe identificative dei partecipanti alla rete. Il *PPR* è il contratto che viene stipulato tra due nodi della rete[159]. Un nodo funge da archivio e gestore della documentazione dell'altro. In pratica sono presenti, a titolo di esempio, i nodi A e B dove A è il provider delle informazioni e B, invece, è il nodo al quale appartengono i dati. Il contenuto del *PPR* è costituito dall'assortimento dei dati e delle relative autorizzazioni trattenute presso il fornitore di assistenza, ossia il *care provider.* Ogni *pointer* corrisponde ad una stringa della domanda, la quale qualora venisse eseguito lo smart contract nel database del provider, produce come risultato un sottoinsieme dei dati del paziente. Ogni stringa può specificare quale porzione di dati del paziente si voglia condividere con terze parti. Infine il *Summary Contract* riassume il contenuto del *PPR*. Il *Summary Contract*, oltre a presentare le interazioni che si sono avute nella blockchain, provvede anche alle notifiche di sistema. Notifiche che si hanno nel momento in cui il provider va ad aggiornare la documentazione riguardante il paziente o quando viene creata una nuova relazione. A seguito di tali operazioni, il diretto interessato riceve una notifica ed egli può decidere se accettare, rigettare o porre fine alla relazione con il provider[160]. Il funzionamento di MedRec è piuttosto complesso e tale complessità è dovuta alla presenza di quattro elementi, ossia: (i) il *Backend Library,* (ii) *Ethereum Client,* (iii) il *Database Gatekeeper* e (iv) l'*EHR Manager*[161]. Nel momento in cui vi è la registrazione di un nuovo paziente viene utilizzato il Registrar Contract. L'identità del nuovo arrivato viene associata a quella del suo indirizzo su Ethereum e il Summary Contract corrispondente viene creato. Il provider, successivamente, carica sulla rete un nuovo *Patient-Provider Relantionship Contract* e crea una stringa di domanda come punto di riferimento. Il nodo, dunque, invia la transazione che collega il *PPR* al *Summary Contract* consentendo al peer che fa riferimento al paziente di essere allocato nella blockchain. Il secondo elemento, invece, gestisce le operazioni che avvengono nella blockchain. Si è giunti al punto in cui viene creato un nuovo blocco grazie al *Patient – Provider Relantionship Contract*. L'utente riceve una notifica ed egli può accettare o declinare la comunicazione con il provider. Se l'utente accetta, MedRec invia una stringa di domanda per poter ottenere nuove informazioni. Il terzo elemento, ossia il *Database Gatekeeper*, è l'interfaccia off-chain. È il database che gestisce le richieste

[158] Azaria, Ekblaw, Vieira , & Lippman, 2016
[159] *Ibidem*
[160] *Ibidem*
[161] *Ibidem*

effettuate al server. Il paziente, dunque, seleziona i dati e gli aggiornamenti che intende condividere nel *PPR* con la terza parte. La terza parte riceve una notifica circa i nuovi permessi e può seguire il link per ottenere tutte le informazioni di cui ha bisogno. Infine, vi è il gestore dei referti online, ossia l'*Electronic Health Record Manager,* il quale permette l'accesso ai dati tramite un'interfaccia web e tramite applicazione su mobile. Da questa sommaria descrizione, si comprende come il funzionamento non sia semplice e come la blockchain e gli smart contract siano alla base di questo meccanismo. L'elemento caratterizzante MedRec è l'essere *source agnostic*[162]*,* ossia la possibilità di recepire informazioni da qualsiasi database e provider in assenza di ostacoli che impediscono la condivisione dei dati andando, così, a porre rimedio al problema dell'interoperabilità. La tecnologia blockchain trova applicazione anche nel settore farmaceutico, strettamente correlato a quello sanitario, con due obiettivi principalmente: migliorare la catena di approvvigionamento, in quanto le supply chain sono sempre più complesse nella loro organizzazione[163] garantendo una tracciabilità dei farmaci più precisa ed efficiente e diminuire la contraffazione e il contrabbando di farmaci. Chronicled[164] a tal proposito offre come soluzione MediLedger, il quale utilizza Hyperledger Fabric. Il suo funzionamento non è immediato, in quanto MediLedger è composto da diversi elementi. Nei cc.dd. *chaincodes,* ossia gli smart contract utilizzati in Hyperledger Fabric, sono presenti tre tipologie di smart contract a cui viene data esecuzione nella blockchain, cioè (i) il *Drug Registration Contract*, (ii) il *Consignment Accumulation Contract* e (iii) il *Transaction Update Contract*. Il *Drug Registration Contract* è il contratto che viene stipulato tra il fornitore e il produttore utilizzato per la registrazione di un nuovo prodotto e le sue componenti. Il *Consignment Accumulation Contract*, invece, viene utilizzato nel momento in cui un nuovo farmaco viene registrato nel *Drug Registration Contract*. Infine, il *Transaction Update Contract* viene impiegato nel momento in cui vi è una nuova informazione che viene aggiunta al *Consignment Accumulation Contract*. I due contratti, infatti, sono strettamente correlati tra loro. L'informazione che viene aggiornata e archiviata tramite il TUC[165] include il valore di hash della transazione presente e di quella precedente, il valore di hash del mittente e dell'indirizzo del destinatario e il marcatore temporale[166]. La tracciabilità dei farmaci, dunque, avviene su MediLegdger tramite l'utilizzazione di questi tre smart contract che interagiscono tra di loro. Il funzionamento di MediLedger può essere riassunto nel seguente modo. Nel momento in cui viene registrato un nuovo farmaco e i suoi componenti una proposta di transazione viene trasmessa a

[162] *Ibidem*
[163] Uddin, 2021
[164] Azienza a cui fa riferimento MediLedger che ha come obiettivo di fornire supporto al network MediLedger per facilitare la fiducia e abilitare l'automazione tra partner commerciali. Tratto da: https://www.chronicled.com/about-us
[165] Acronimo per Transaction Update Contract.
[166] Uddin, 2021

MediLedger, il quale la trasmetterà a tutti i nodi della rete. Una volta eseguita, il risultato viene crittografato e registrato assieme alla firma digitale dei nodi di approvazione. L'approvazione, dunque, viene inviata al mittente della transazione come risposta alla sua proposta. Successivamente il nodo che fa capo al produttore riunisce tutte le approvazioni ricevute per trasmetterle all'ordering service e aggiungerle alla blockchain[167]. Traendo qualche conclusione, è evidente come la tecnologia blockchain possa essere applicata nel settore sanitario, ma è altrettanto chiaro come la ricerca in questo ambito sia ancora agli inizi. Anche se si è consapevoli delle potenzialità che tale tecnologia offre, quali transazioni più veloci e il venir meno del problema dell'interoperabilità permangono ancora alcuni ostacoli che devono essere superati per poter auspicare, in futuro, un'implementazione della blockchain nella sanità digitale. Le difficoltà che rendono difficile tale operazione si possono individuare in due categorie: resistenza culturale al cambiamento e mancanza di standard e regolamentazione da parte del Legislatore. Gli operatori sanitari e le aziende ospedaliere sono restie al cambiamento e all'adozione di una tecnologia che, per quanto non del tutto sconosciuta, non è del tutto immediata nella sua utilizzazione. Questo fa sì che gli operatori sanitari siano privi delle conoscenze base, per cui è necessario che ricevano una formazione adeguata al fine di usufruire degli strumenti forniti da tale tecnologia. Tutto questo, però, richiede investimenti che non si è ancora disposti ad effettuare proprio perché vi è un'incertezza circa l'*outcome* di queste tecnologie applicate al settore sanitario. La ricerca, si diceva, è ancora agli inizi e servirebbero ulteriori dati, informazioni, risultati per iniziare a considerare l'investimento di ingenti somme sia nella formazione del personale sia nelle infrastrutture. Le infrastrutture di cui si è dotati, infatti, risultano essere insufficienti per un'implementazione, ad oggi, della blockchain. La resistenza culturale al cambiamento, inoltre, non è solo dalla parte dell'operatore sanitario ma anche del paziente. L'uomo comune avrà sicuramente sentito parlare di blockchain, ma non ne comprende il funzionamento. Vi è, quindi, la necessità anche in questo caso di una educazione digitale al fine di comprendere al meglio i fondamenti delle nuove tecnologie. Le difficoltà non si ravvisano solo in una certa resistenza al cambiamento da parte dei professionisti del settore e del pubblico, ma anche da parte del Legislatore. Non sono presenti, infatti, testi normativi in materia che disciplinano l'utilizzazione della blockchain. L'assenza di una disciplina di carattere generale in un testo di legge trova fondamento nel fatto che tali tecnologie sono in continuo sviluppo, per cui sarebbe necessario un intervento continuo da parte del Legislatore andando, conseguentemente, ad emendare i testi di legge. I continui emendamenti, a lungo andare, non beneficiano né i cittadini né gli operatori economici, in quanto il testo risulta essere di difficile comprensione con l'aggiunta di nuovi commi che vanno ad allungare, inutilmente, il testo di riferimento. Non sono presenti solo

[167] *Ibidem*

problemi a livello di comprensione, ma anche di certezza del diritto. Una continua modifica alla disciplina rende difficile capire quale sia quella vigente e quale, invece, non debba essere più seguita in quanto abrogata da quella in vigore. Essendo presenti queste difficoltà sarebbe auspicabile l'emanazione di linee guida o di raccomandazioni che, non essendo vincolanti, si adattano meglio a tale contesto. La presenza, dunque, di questi testi di carattere generale inoltre porrebbe rimedio anche ad un'ulteriore problema, ossia la mancanza di standard. Non sono, infatti, presenti standard comuni circa, ad esempio, la tipologia di dati che possono essere archiviati nella rete o la grandezza di essi o il format con il quale devono essere registrati. L'utilizzazione di linee guida e di raccomandazioni potrebbe, dunque, porre rimedio a questo problema andando ad individuare le specifiche che devono essere comuni a tutte le blockchain utilizzate in questo settore. In conclusione, la blockchain è sicuramente una risorsa preziosa che può trovare applicazione in diversi ambiti della quotidianità. Potrebbe, però, essere necessario ancora del tempo prima che venga implementata in settori diversi da quello per il quale è stata originariamente progettata, ossia quello finanziario a causa degli ostacoli ancora presenti che ne rendono difficile l'applicazione in concreto.

5. Datificazione e blockchain: l'aspetto politico – utopistico.

Il mondo contemporaneo è immerso nella produzione e nella raccolta di dati e in questo contesto nasce il concetto di datificazione. Per datificazione si intende l'elaborazione di eventi in dati, ossia in rappresentazioni simboliche manipolabili, che vengono riorganizzati e utilizzati per estrarre conoscenza in riferimento all'ambito esaminato[168]. La datificazione, dunque, è uno dei tanti linguaggi di interpretazione della realtà circostante. Più precisamente si tratta del ciclo della datificazione, ossia di una sequenza in eventi – dati – conoscenza – decisione – azione – eventi[169]. Nello specifico, l'evento è una qualsiasi manifestazione captabile nella realtà. Ad esempio, per evento si intende una fotografia che cattura un determinato momento rendendolo indelebile. Dall'evento emerge il dato, ossia una struttura simbolica manipolabile dal quale è possibile estrarre conoscenza. Un esempio di conoscenza estratta dai dati immessi nella infosfera[170] è la pubblicità di un prodotto sui diversi canali social. Le grandi aziende, infatti, osservano le abitudini digitali dei potenziali clienti, per esempio, i like e le condivisioni, per poter poi piazzare, in gergo *placement,* la pubblicità del loro prodotto e tutto ciò è reso possibile grazie alla raccolta e l'elaborazione dei dati. Una volta estratta la conoscenza è possibile

[168] Sarra, 2022
[169] *Ibidem*
[170] Per infosfera si intende *l'insieme dei mezzi di informazione e comunicazione, e il complesso delle informazioni che circolano attraverso questi mezzi.* Tratto da: https://www.garzantilinguistica.it/ricerca/?q=infosfera

prendere una decisione, la quale porta, poi, ad un'azione che a sua volta farà ricominciare il ciclo della datificazione. La datificazione presenta diversi aspetti e, ai fini della trattazione, il profilo che risulta essere più compatibile con la blockchain è quello politico – utopistico che richiama alcuni principi dell'etica hacker come la cultura *open source,* la condivisione e la decentralizzazione[171]. Si iniziò a parlare di cultura *open source,* ossia di sorgente aperta, negli anni '80 del secolo scorso grazie a Richard Stallman uno degli autori del primo sistema operativo libero, ossia il progetto GNU[172]. La filosofia di Stallman si basa su quattro libertà, ovvero (i) la libertà di eseguire il programma come si desidera e per qualsiasi scopo, (ii) la libertà di studiare il codice sorgente e modificarlo, (iii) la libertà di creare e distribuire copie del programma ed infine (iv) la libertà di creare e distribuire versioni modificate del programma stesso[173]. L'integrazione di questi principi e dell'etica hacker nella datificazione contribuisce alla realizzazione del progresso tecnologico e in tale ambito si inserisce anche la blockchain. Affinché si possa concretizzare la visione politico – utopistica della datificazione è necessario il soddisfacimento di tre condizioni. La prima prevede l'accesso a dati grezzi. Per dato grezzo si intende il dato che non è stato ancora processato, dunque da esso non è stata ancora estratta conoscenza. La seconda condizione è la presenza di strumenti di partecipazione tecnologica. Ci si riferisce alle tecnologie civiche, quali, ad esempio le piattaforme adibite al voto elettronico. Grazie a tali strumenti risulta possibile al cittadino partecipare in maniera più attiva e consapevole ai processi decisionali. Dal momento che le tecnologie civiche a disposizione non sono di immediato utilizzo, la terza condizione pone la presenza di intermediari, ossia di soggetti dotati di *know how,* quindi di conoscenze base, che sono in grado di rendere accessibile la partecipazione del popolo alla vita politica[174]. Tra i presupposti che riguardano il profilo politico – utopistico, la presenza di strumenti di partecipazione tecnologica è la più rilevante per il legame tra datificazione e blockchain. Con riferimento a tale presupposto, le tecnologie civiche potrebbero usufruire della blockchain per garantire processi elettorali più trasparenti, sicuri e rapidi. L'utilizzazione di tali tecnologie, poi, consentirebbe una maggior partecipazione dell'elettorato ai processi decisionali, il che comporta all'*empowerment* del singolo, andando, dunque, a realizzare quanto prospettato nella visione politico – utopistica della datificazione. La tecnologia, infatti, non deve essere considerata come elemento negativo, vale a dire come strumento in mano a pochi eletti che sono in grado di modificare la realtà a loro piacimento per controllare le masse, ma come mezzo per contrastare il potere stesso. In tal senso, dunque, si parla di *empowerment* inteso come potenziamento, autonomizzazione rispetto ad un altro soggetto. Tale

[171] Sarra, 2022
[172] Tratto da https://www.gnu.org/gnu/thegnuproject.it.html
[173] Tratto da https://www.gnu.org/philosophy/free-software-even-more-important.it.html
[174] Sarra, 2022

risultato, del tutto utopico, sarebbe raggiungibile grazie all'impiego di tecnologie, anche nell'ambito del voto. Ciò permetterebbe, infatti, di realizzare in concreto la democrazia diretta, ossia consentendo ai cittadini di partecipare attivamente alla vita politica del Paese senza la necessità di nominare intermediari, ossia loro rappresentanti. Per chiudere il cerchio, quindi, datificazione e blockchain sono correlate tra loro in quanto la blockchain si inserisce sotto il profilo politico – utopistico rendendo, idealmente, possibile la visione che tale aspetto pone. È un'utopia, ma non è da escludere che in futuro ciò possa effettivamente verificarsi. Una cosa è certa: affinché si concretizzi la visione politica – utopistica della datificazione è necessario un profondo cambiamento culturale che può proprio partire dall'utilizzazione della blockchain nell'ambito del voto. Tale aspetto verrà indagato nei capitoli successivi partendo dalla democrazia elettronica e le cause che hanno portato alla sua concettualizzazione per, poi, passare al voto elettronico esaminando i vantaggi e le criticità dell'applicazione della blockchain in tale settore.

CAPITOLO II: IL CONCETTO DI DEMOCRAZIA.

1. Nozione di democrazia

1.1. Origini della democrazia

Vi è un detto, il quale statuisce che Atene è la culla della democrazia. Un fondo di verità c'è in questa affermazione, in quanto la democrazia nasce proprio ad Atene nel contesto delle *polis* tra il VII e il VI secolo a.C. ed è il frutto di un lungo processo di cambiamenti nella società greca di carattere culturale, politico e tecnologico in riferimento ai progressi nel campo della navigazione e la conseguente intensificazione degli scambi commerciali dovuti, anche, alla fondazione delle prime colonie[175]. Tale forma di governo, però, non è il risultato di un processo pacifico, ma è la conseguenza di violenze e lotte tra diverse classi sociali dimostrando che qualsiasi forma di governo esistente non è stabile, in quanto è sempre presente il rischio di una possibile ribellione da parte dei governati. In particolare, agli arbori della democrazia ateniese vi era la presenza di due fazioni opposte portatrici di interessi contrastanti. Da un lato, infatti, vi erano gli aristocratici i quali, nel frattempo, si erano sostituiti nell'esercizio del potere alle monarchie ormai decadute e dall'altro vi erano le classi popolari espropriate delle loro terre e ridotte in schiavitù a causa dell'impossibilità di saldare i debiti contratti. In questo contesto si sviluppa la polis, ossia la città-stato la quale, in origine, è un agglomerato di villaggi che si sono poi uniti per formare grandi centri urbani. Tale processo di unificazione fu promosso dalle famiglie aristocratiche, le quali nel frattempo si erano arricchite grazie all'attività agricola svolta nei loro possedimenti terrieri[176]. Con la *polis,* poi, vi furono delle importanti riforme di carattere amministrativo e giudiziario che contribuirono a dar forma alla democrazia ateniese andandone a costituire l'assetto istituzionale. Un ulteriore fattore che ha permesso l'affermarsi della democrazia, oltre alle tensioni sociali e alla nascita della *polis*, è la riscoperta dell'alfabeto[177]. A seguito della caduta di Micene, avvenuta nel XIII secolo a.C., si apre il cc.dd. Medioevo ellenico periodo buio, in quanto sono quasi del tutto assenti reperti archeologici e testi scritti che provano lo splendore di questa epoca. Solo a partire dal VII secolo a.C. grazie ai poemi Omerici si chiude questo periodo buio per fare spazio al Rinascimento ellenico, infatti grazie all'Iliade e all'Odissea la civiltà greca riscopre l'alfabeto e la scrittura. L'alfabeto e la scrittura sono gli strumenti che hanno contribuito

[175] Marchettoni, 2018
[176] Tratto da https://www.storicang.it/a/nascita-della-polis-trasforma-grecia_15848
[177] Gauthier, 2023

all'affermazione della democrazia nella *polis,* poiché per la prima volta vengono messe per iscritto le leggi che governano la città – stato ponendo fine all'oralità. Grazie a tale riscoperta nasce il principio di legalità, uno dei principi cardine delle democrazie contemporanee. La scrittura è l'antidoto contro il potere degli aristocratici che fino a quel momento erano gli unici che fossero in grado di stabilire che cosa fosse giusto e che cosa fosse sbagliato[178]. Gli aristocratici di Atene erano consapevoli dell'assenza della parola scritta e di come questo fosse un enorme vantaggio, in quanto risultava più agevole indicare al *demos* quale fosse il comportamento da tenere e quale da evitare e come fosse più semplice alterare tali precetti. La parola scritta, invece, impedisce il verificarsi di tale situazione, dunque, è chiaro come la scrittura sia stata un elemento cruciale nella riduzione del potere d'influenza degli aristocratici sul *demos.* Il tutto si può riassumere nel proverbio latino *verba volant, scripta manent* ossia le parole volano, ma quelle scritte rimangono.

Al di là di questi fattori di carattere sociale e culturale, non è semplice dare una definizione appropriata di democrazia. È noto come il termine derivi dal greco *demos,* ossia popolo o comunità inteso in senso più ampio e *kratos,* lemma che assume il significato di potere. Unendo questi due elementi, democrazia significa autogoverno del popolo, ossia i cittadini sono in grado di prendere decisioni direttamente senza la necessità di nominare dei rappresentanti che ne facciano le veci e che decidano per loro. Si può, quindi, affermare come la democrazia ateniese sia la prima esperienza nella storia di democrazia diretta.

Durante la fase di consolidamento, le riforme di Solone del VI secolo a.C. di carattere politico e sociale hanno posto le basi per la formazione dell'assetto istituzionale della democrazia ateniese[179]. Dal punto di vista delle riforme, la più rilevante è quella sociale poiché grazie alla suddivisione del censo in pentacosiomedimni, cavalieri, zeugiti e teti[180] si è evitata una possibile frattura tra ricchi, ossia gli aristocratici proprietari terrieri, e i poveri divenuti schiavi a causa dei debiti contratti. Con lo scopo, poi, di indebolire il potere degli aristocratici cercando, quindi, di far sì che ognuno potesse contribuire al governo della *polis* in base alle proprie capacità contributive, Solone pose fine alla schiavitù per debiti e ridusse i poteri dell'Areopago, ossia il tribunale più antico dell'Ellade composto dagli arconti, i quali si occupavano di reati particolarmente gravi, quali, ad esempio l'omicidio. La democrazia ateniese, per come è conosciuta oggi, si è affermata e consolidata

[178] *Ibidem*

[179] Tra le riforme più importanti si possono citare l'abolizione delle ipoteche sui terreni dei contadini - la cc.dd. *seisàchtheia,*- e il divieto di esportare prodotti agricoli per favorire le classi di censo meno abbienti. Tratto da: Universale, la grande enciclopedia tematica, 2005

[180] I primi sono coloro che hanno un reddito di almeno cinquecento medimni di cereali o metreti di olio e vino, i secondi hanno un reddito di trecento unità, gli zeugiti detengono almeno 200 unità, infine i teti sono la classe di censo più povera con un reddito inferiore a duecento medimni di cereali o metreti di olio e vino. Tratto da: Universale, la grande enciclopedia tematica, 2005

con Clistene e le sue riforme a partire dal 510 a.C. Dal punto di vista sociale, con Clistene le quattro tribù istituite da Solone vennero abolite e i cittadini furono suddivisi in dieci tribù territoriali[181]. Dal punto di vista politico Clistene diede vita all'*ecclesia,* alla *bulè,* alla *pritania,* alle magistrature e ai tribunali popolari[182] andando, così, a costituire l'assetto istituzionale democratico della Grecia antica pervenuto fino ai giorni nostri. Gli organi più interessanti che permettono di comprendere come funzionasse la democrazia nell'Atene del V secolo a.C. sono l'*ecclesia,* ossia l'assemblea dei cittadini e la *bulè,* ovvero il consiglio dei Cinquecento. Per *ecclesia* si intende l'assemblea del popolo che veniva convocata per decidere le questioni più importanti riguardanti la *polis*[183]. Chi vi partecipava era il popolo inteso nel senso di cittadini, i quali erano individui di sesso maschile, con più di vent'anni e con padre ateniese[184]. Tali requisiti comportavano una restrizione del suffragio, infatti anche se democrazia significa autogoverno del popolo ciò non implica tutto il popolo, ma solo una parte di esso. Rimanevano, infatti, esclusi le donne, i bambini, gli schiavi e gli stranieri. Potere al popolo e del popolo, ma non a tutti. Nonostante vi fosse un suffragio assai ristretto, l'importanza dell'*ecclesia* emerge in riferimento alle questioni su cui si esprimeva ossia (i) l'elezione dei magistrati e il controllo della loro attività, (ii) la politica interna ed estera, e (iii) le deliberazioni in ambito legislativo, amministrativo e finanziario[185]. L'assemblea, dunque, deliberava su questioni di fondamentale importanza per la comunità, per cui si comprende come avesse un ruolo assai rilevante. Si può osare ad affermare come l'*ecclesia* fosse addirittura più importante della *bulè,* in quanto racchiudeva la popolazione ed era espressione della sua volontà. All'*ecclesia* vi partecipavano sia i cittadini appartenenti alle classi più ricche sia coloro che, invece, rientravano nelle classi di censo più povere. È evidente come per i più poveri fosse quasi impossibile prendere parte a tutte le deliberazioni dell'*ecclesia*, in quanto per le classi più modeste la priorità non era la partecipazione all'assemblea e l'esercizio della *politeia,* ossia dei diritti e dei doveri di cittadino, ma guadagnarsi da vivere lavorando. Per tale ragione, allo scopo di favorire la presenza delle classi meno abbienti venne istituito il *misthos ekklesiastikos*, ossia lo Stato pagava al cittadino la giornata di lavoro persa per poter prendere parte all'*ecclesia*[186].

La *bulè* rappresenta il consiglio dei Cinquecento essendo costituita da cinquecento membri di età superiore a trent'anni ed estratti a sorte tra i candidati di ognuna delle dieci tribù locali. Chi faceva

[181] Ad esempio, la regione di Atene, ossia l'Attica, venne frazionata in tre aree: città, costa e zone interne. Ciascuna di esse fu ripartita in *demi* e ogni tribù era costituita da un numero variabile di *demi.* Vi fu, quindi, un cambiamento circa l'assetto sociale con lo scopo del rimescolamento della cittadinanza. Si veda Marchettoni, 2018
[182] Marchettoni, 2018
[183] Tratto da Universale, la grande enciclopedia tematica, 2005
[184] Da Pericle in poi per poter godere dello status di cittadino sarà necessario avere madre e padre ateniesi.
[185] Universale, la grande enciclopedia tematica, 2005
[186] Universale, la grande enciclopedia tematica, 2005

parte della *bulè* non poteva ricoprire tale incarico per più di due volte nell'arco della vita. I compiti erano molteplici, tra cui (i) l'esame delle proposte dei magistrati, (ii) l'elaborazione dei disegni di legge da sottoporre all'*ecclesia* e (iii) funzioni di polizia e di giustizia riguardanti la giurisdizione penale circa il delitto di alto tradimento e reati contro lo Stato[187].

Tale è, quindi, l'assetto della democrazia ateniese che durerà fino alla crisi iniziata con la guerra del Peloponneso[188] tra Atene e Sparta che risulterà essere una delle guerre più sanguinarie della storia dell'Ellade e la conquista macedone della Grecia da parte di Filippo II nel 332 a.C. Come ogni forma di governo, anche la democrazia ha vissuto momenti di massimo splendore e momenti di crisi che l'hanno portata ad un lento e inesorabile declino. La forma di governo democratica è la più diffusa, ma si può pacificamente affermare come le democrazie contemporanee abbiano pochi elementi in comune con il modello originario. Ciò che è certo è il recepimento di alcuni principi fondamentali, quali il principio di legalità, il principio di uguaglianza davanti alla legge e la libertà di espressione.

1.2. Che cos'è la democrazia oggi

Nel paragrafo precedente si è fatto un breve excursus storico sull'origine della democrazia avendo come modello di riferimento la democrazia ateniese del V secolo a.C. in quanto è la prima forma di democrazia che il mondo Occidentale abbia conosciuto, oltre ad essere la più documentata.

Ad oggi, la democrazia è la forma di governo maggiormente diffusa ma oltre al nome e al recepimento di alcuni principi fondamentali non vi è nient'altro in comune con la democrazia ateniese. Se si dovesse dare una definizione di democrazia, tale compito risulterebbe essere assai arduo in quanto tale termine è connotato da una incertezza nella definizione, poiché a democrazia viene associato uno specifico aggettivo in funzione del tema trattato, dunque, viene meno il nucleo centrale della definizione[189].

La forma di democrazia prevalente è di tipo rappresentativo, ossia i cittadini tramite l'esercizio del diritto al voto eleggono i rappresentanti che ne fanno le veci nelle sedi istituzionali e che dovrebbero incarnare gli interessi di coloro che gli hanno eletti. Bisogna ricordare che nella nostra Costituzione all'art.67[190] è previsto il divieto di mandato imperativo, ossia il parlamentare una volta eletto è libero di esercitare le proprie funzioni, pertanto non ha obblighi nei confronti del partito di appartenenza né nei confronti del programma elettorale e degli elettori. Sembra un controsenso, data la definizione di democrazia rappresentativa, in realtà vi è una forma di responsabilità di carattere politico, in quanto il

[187] Universale, la grande enciclopedia tematica, 2005

[188] Guerra combattuta tra il 431 a.C. e il 404 a.C. che vedeva due fazioni contrapposte, ossia la lega peloponnesiaca con a capo Sparta e Atene leader della lega delio attica.

[189] Gallo, 2020

[190] Il quale statuisce: "*Ogni membro del Parlamento rappresenta la Nazione ed esercita le sue funzioni senza vincolo di mandato".*

parlamentare risponderà in sede elettorale venendo giudicato dagli elettori con la rielezione o con l'elezione di un rappresentante diverso. È fondamentale la presenza del divieto del mandato imperativo, in quanto un mandato vincolante, il quale implicherebbe un obbligo per il parlamentare di rimanere fedele alle promesse fatte in campagna elettorale oppure il ricevere e attenersi agli ordini e alle direttive del partito, significherebbe eliminare il cuore della democrazia rappresentativa, ossia il Parlamento luogo di dibattito e continuo confronto tra maggioranza e opposizione. Se ci fosse un mandato vincolante, dunque, non vi sarebbe lo spazio per la mediazione con le forze politiche opposte[191]. Lo scopo di questa forma di governo è perseguire gli interessi dei rappresentati e giungere alla decisione *migliore* per la collettività. Ciò è garantito dai partiti politici i quali sono espressione del pluralismo. Non si nega, però, la crisi della democrazia rappresentativa causata da una serie di fattori, tra cui una scarsa fiducia dei governati nei confronti della classe politica che non rappresenta più gli interessi di chi gli ha eletti, le crisi economiche che si presentano ciclicamente e un mutamento che riguarda la struttura del partito stesso. Non si tratta più, infatti, di un partito coeso facilmente incasellabile in destra o sinistra, ma iperpersonalizzato ponendo l'attenzione sulla figura del leader di partito[192]. Oltre alla democrazia rappresentativa di recente è emerso il concetto di tecnocrazia. Nella tecnocrazia, l'Esecutivo viene affidato provvisoriamente a soggetti specializzati in vari settori, come quello economico e sociale, per fronteggiare una situazione emergenziale. Il Governo dei tecnici, dunque, è composto da individui che non hanno estrazione di carattere politico. Un esempio di tecnocrazia è la recente esperienza vissuta con l'epidemia da SARS-CoV-2. Le decisioni circa i *lockdown*, le zone rosse, arancioni e gialle sono state prese da tecnici, ossia da esperti in materia come infettivologi e virologi. Bisogna considerare come tale particolare forma di governo debba venire in auge solo in extremis, in quanto vi è una totale delegittimazione dei tecnici da parte del popolo che viene governato da soggetti che prendono decisioni in sua vece senza essere stati eletti. Si potrebbe paragonare la tecnocrazia ad una sorta di dittatura facendo riferimento non al concetto di dittatura odierna, ma all'istituto di diritto romano. Anche l'antica Roma conosceva un governo tecnico, attribuendo in situazioni di particolare crisi o di emergenza ad un magistrato l'*imperium maximum*, ossia la pienezza dei poteri civili e militari[193] per un periodo limitato di massimo sei mesi.

Un ulteriore evoluzione del concetto di democrazia, poi, deriva dalle più recenti riflessioni di carattere politico – giuridico che prendono coscienza del fatto che vi possa essere l'utilizzazione della tecnologia e delle ICT nei processi di partecipazione politica e decisionali, per tal ragione si parla di democrazia

[191] Gallo, 2020

[192] Tale cambiamento si è riscontrato con la fine della cc.dd. Prima Repubblica e l'ascesa in politica di Silvio Berlusconi e del suo partito Forza Italia. Essendo poi agli inizi della Internet Revolution vi era in atto un profondo mutamento nel modo di relazionarsi con il corpo elettorale che ha segnato una nuova era della comunicazione tra corpo politico ed elettori.

[193] (Enciclopedia Treccani, voce dittatore.

elettronica. La democrazia elettronica è un concetto che è stato elaborato a seguito della crisi della democrazia rappresentativa come possibile alternativa affinché venga ristabilita la fiducia da parte dell'elettorato nelle istituzioni. Per poter raggiungere questo risultato, dunque, è necessario instaurare un continuo dialogo tra elettorato e classe politica. Dialogo che si può instaurare sfruttando i canali social entrando, quindi, in diretto contatto con la propria fetta di pubblico, ma anche tramite mezzi più sofisticati e formali, quali sondaggi o questionari. Sono tutti mezzi che permettono di ottenere un riscontro diretto su quali siano le esigenze dell'elettorato e le problematiche riscontrate che permetterebbero un maggior coinvolgimento della popolazione nei processi decisionali non solo in prossimità delle elezioni, ma anche nelle fasi antecedenti. In estrema sintesi la democrazia elettronica prevede l'utilizzazione della tecnologia e delle ICT *strumentali all'adozione di decisioni collettive*[194] con l'obiettivo di ristabilire un rapporto di fiducia con l'elettorato e ottenere una maggiore partecipazione ai processi decisionali. Una riflessione, poi, deve essere effettuata circa il fenomeno della cc.dd. democrazia illiberale. Il concetto di democrazia illiberale non è semplice da definire. Si può affermare come formalmente vi sia un regime democratico, ma sostanzialmente vi sono delle importanti modifiche nell'assetto istituzionale tali per cui vi è una compressione di quelli che sono i valori e i principi della democrazia liberale. La democrazia illiberale, dunque, si connota per una serie di caratteristiche che rendono tale fenomeno alquanto peculiare. In primis, vi è una progressiva compressione del principio della separazione dei poteri, questo perché l'Esecutivo si fa diretto interlocutore con il popolo, mentre nelle democrazie liberali è il Parlamento che rappresenta la volontà popolare, dunque il ruolo predominante dell'Esecutivo sortisce l'effetto di erodere sempre di più la funzione rappresentativa[195] del Parlamento andando di conseguenza a indebolire il principio della separazione dei poteri. Tale principio, poi, è ulteriormente compromesso nel rapporto tra il potere esecutivo e la giustizia costituzionale. Per esempio, in Ungheria vi è stata l'approvazione e l'entrata in vigore di una nuova Costituzione nel 2011 la quale ha aumentato il numero dei giudici costituzionali nominati da una commissione parlamentare ed è stato esteso la durata del loro mandato[196]. Si è di fronte ad un paradosso, in quanto un maggior numero di giudici costituzionali e un aumento della durata dell'incarico dovrebbero essere indici di una maggior garanzia di tutela a livello costituzionale. In realtà, a fronte di questo aumento di carattere quantitativo è stato posto un limite delineato dall'età pensionabile, ossia sessantadue anni, che ha provocato un ricambio dei giudici facendo sì che fossero nominati giudici più affini con le linee del Governo[197]. L'Esecutivo, dunque, risulta essere

[194] Gometz, 2017
[195] Milani, 2019
[196] Raniolo, 2020
[197] *Ibidem*

predominante rispetto ai poteri legislativo e giudiziario. Sul tal punto, quindi, è naturale concentrare l'attenzione sull'indebolimento dei meccanismi di responsabilità politica, la quale può essere di carattere elettorale o interistituzionale[198], presenti invece nelle democrazie liberali. Per responsabilità elettorale si intende il giudizio dei cittadini alle elezioni per cui il capo di Governo e il suo partito possono essere rieletti o meno, essi, dunque, danno conto di quanto è stato fatto e di quanto non è stato fatto durante il mandato. Per responsabilità interistituzionale, invece, si fa riferimento alle interrogazioni parlamentari a cui gli esponenti del Governo possono essere sottoposti in presenza di questioni controverse[199]. Ulteriore elemento caratteristico della democrazia illiberale è la progressiva riduzione delle libertà fondamentali, come la libertà di pensiero. Difatti, è capillare il controllo dei media e dei canali di comunicazione da parte dell'Esecutivo giungendo, in casi estremi, alla censura di alcune espressioni o parole chiave in Rete che consentirebbero, invece, alla cittadinanza di accedere ad un portale di informazioni che presenta una narrativa diversa rispetto a quella dello Stato. Sono casi estremi che pur però si possono verificare. Non è semplice, quindi, comprendere se si è dinnanzi o meno ad una cc.dd. democrazia illiberale, pertanto una delle strategie per poter comprenderne al meglio le caratteristiche consiste nel ricercare gli elementi tipici della democrazia liberale[200] e constatare se siano presenti o meno. Qualora dovesse esserci un difetto di alcuni elementi, come la separazione dei poteri o la progressiva compressione dei diritti fondamentali, vi è il rischio, o perlomeno il sentore, di trovarsi dinnanzi ad una forma democratica illiberale.

Emerge, dunque, una povertà nel linguaggio ma una varietà di gradazioni del concetto di democrazia. Se si volesse effettuare un confronto tra il modello ateniese e le democrazie contemporanee è possibile affermare come siano presenti delle similitudini, ma anche delle differenze. In primis, grazie alla riscoperta dell'alfabeto e della scrittura nell'Atene arcaica nasce il principio di legalità con la messa per iscritto delle leggi che governavano la città – stato. Nelle democrazie contemporanee, il principio

---

[198] *Ibidem*

[199] Il Parlamento – nell'ordinamento italiano - oltre ad esercitare la sua legislativa, è titolare di funzioni di indirizzo e controllo nei confronti del Governo, in quanto tra Parlamento e Governo persiste un rapporto di fiducia che si tramuta in quella che è la mozione di fiducia sul programma di Governo. In presenza di un fatto o di una questione controversa è possibile che vi sia un'interrogazione parlamentare, ossia domande rivolte agli esponenti di Governo affinché venga fatta chiarezza sul punto. Le domande possono essere poste in forma orale o scritta e le risposte possono essere orali o scritte, immediate o differite oppure non esserci in quanto non vi è un obbligo specifico di risposta.

[200] Tradizionalmente , la forma di Stato liberale si afferma con la progressiva emersione della classe borghese nel XIX secolo, tant'è che viene anche chiamato Stato monoclasse. I connotati principali dello Stato liberale si individuano nella presenza di (i) uno Stato minimo, ossia uno Stato basato sul principio del *laissez-faire*, tale per cui vi è un intervento minimo dello Stato nelle attività dei privati, (ii) l'affermazione della separazione dei poteri in netto contrasto con lo Stato assoluto, perciò i poteri legislativo, esecutivo e giudiziario vengono affidati da tre *soggetti* diversi, (iii) l'affermazione del principio di legalità con il quale si intende che tutti gli atti o i comportamenti dei pubblici poteri devono essere previsti da una legge ed essere conformi ad essa, (iv) dal principio di legalità deriva il principio di uguaglianza in senso formale in base al quale tutti sono uguali davanti alla legge, pertanto non possono esserci discriminazioni basate sulle condizioni sociali, economiche o di altro tipo ed infine (v) il principio rappresentativo in base al quale almeno una Camera del Parlamento è composta da rappresentanti del corpo sociale. Si veda Cuolo, 2019.

di legalità è ciò che caratterizza il cc.dd. Stato di diritto, ossia una forma di Stato il cui fine è quello di controllare e limitare il potere statuale attraverso norme giuridiche generali e astratte[201]. Vi è, poi, da considerare la partecipazione del *demos* ai processi decisionali che si traduce in un suffragio molto limitato. Come detto in precedenza, solo gli individui di sesso maschile con più di vent'anni e con nativi ateniesi potevano partecipare all'*ecclesia.* Vi è in questo una somiglianza, in quanto, prima della conquista del suffragio universale, la partecipazione ai processi decisionali e il diritto al voto erano limitati da alcuni criteri, quali, ad esempio il censo e il livello di alfabetizzazione. Sempre per quanto riguarda il profilo della partecipazione bisogna ricordare come la prima democrazia al mondo fosse diretta, per cui il popolo decideva in assenza di intermediari, mentre ad oggi il modello maggiormente diffuso è di tipo rappresentativo nel quale sono presenti anche alcuni strumenti di democrazia diretta come il referendum o l'iniziativa legislativa popolare. Infine, le democrazie contemporanee recepiscono due principi fondamentali presenti nell'Atene arcaica, ossia l'isonomia e l'isegoria. Per isonomia si intende l'uguaglianza di tutti i cittadini davanti alla legge. L'isonomia, dunque, è l'odierna *rule of law.* Nell'Atene del VI secolo a.C. l'uguaglianza dei cittadini davanti alla legge veniva garantita da una serie di fattori tra cui (i) l'elevato numero dei soggetti chiamati ad esercitare la funzione di magistrato, (ii) la presenza di tribunali popolari per cui i giudici erano persone comuni prive di una formazione giuridica, infine (iii) l'organo giudicante veniva formato il giorno stesso delle udienze[202], perciò anche qualora l'imputato avesse intenzione di corrompere l'organo giudicante non ci sarebbe riuscito non conoscendo anticipatamente la composizione dell'organo giudicante. Ai giorni nostri, invece, l'uguaglianza dei cittadini dinnanzi alla legge è garantita non solo dalla imparzialità e terzietà dei giudici[203], ma anche dall'accesso al potere giudiziario attraverso il superamento di un concorso pubblico[204]. L'isegoria nel contesto della democrazia ateniese a cavallo tra il VII e il VI secolo a.C.

[201] Enciclopedia Treccani, voce Stato di diritto.
[202] Papanikos, 2017
[203] Si fa riferimento all'art.111 co.2 della Costituzione il quale statuisce "*Ogni processo si svolge nel contradditorio tra le parti, in condizioni di parità, davanti a un giudice terzo e imparziale. La legge ne assicura la ragionevole durata".* Per terzietà del giudice si intende l'equidistanza dell'organo giudicante dalle parti, mentre l'imparzialità attiene al modo in cui la funzione di organo giudicante viene esercitata, ossia la decisione deve essere immune da interessi o pregiudizi. Tratto da Camon, 2021.
[204] A titolo di esempio faccio riferimento all'attuale modalità di concorso per l'accesso alla carica di magistrato ordinario disciplinata dal Decreto ministeriale del 8 aprile 2024. All'articolo 2 sono previsti una serie di requisiti di ammissione al concorso tra cui godere della cittadinanza italiana e dei diritti civili e avere una avere una condotta incensurabile. L'articolo 5 disciplina la modalità concorsuale specificando che l'esame consiste in una prova scritta, la quale prevede tre elaborati teorici in materia di diritto civile, diritto penale e diritto amministrativo e una prova orale articolata su più materie, tra cui, ad esempio, procedura civile e penale, diritto civile e penale, diritto commerciale e fallimentare ed elementi di informatica giuridica e di ordinamento giudiziario. L'articolo che è di più rilievo e che garantisce una assoluta terzietà nella modalità di svolgimento delle prove, nonché nella scelta dei candidati è l'art.6, il quale disciplina la composizione della commissione esaminatrice. Essa è costituita da (i) un magistrato che abbia conseguito la sesta valutazione di professionalità che svolge la funzione di Presidente della commissione, (ii) da tre magistrati che abbiano conseguito la terza valutazione di professionalità, (iii) da cinque professori universitari di ruolo titolari di insegnamenti nelle materie oggetto di esame e (iv)

era il diritto che godeva ogni cittadino partecipante all'*ecclesia* di prendere parola e parlare liberamente davanti ad un corpo politico, quale l'assemblea dei cittadini. Isegoria nel XXI secolo, però, non coincide con quella della democrazia ateniese, in quanto il suo significato è del tutto diverso. L'isegoria oggi viene tradotta nella libertà di espressione. Il poter liberamente manifestare la propria opinione è una delle conquiste più importanti, soprattutto a seguito dell'esperienza del Ventennio, ed è uno dei principi fondamentali che sorregge la democrazia come conosciuta dal mondo di oggi. Tale libertà può essere esercitata non solo nei luoghi fisici, ma anche in quelli virtuali. A seguito dell'Internet revolution, iniziata negli anni '90 del secolo scorso, la tecnologia è diventata sempre più parte della vita quotidiana dell'uomo moderno. Con la nascita dei social la libertà di espressione si è rafforzata, in quanto chiunque è in grado di esprimere il proprio parere su una determinata questione. Se nel mondo antico l'isegoria veniva esercitata ai piedi della Pnice[205], ad oggi, invece la piazza pubblica è rappresentata dai social network. Anticipando quanto verrà detto nei successivi paragrafi, l'utilizzazione delle ICT e dei nuovi mezzi di comunicazione ha profondamente mutato il significato di democrazia nell'era contemporanea. Internet e i social sono strumenti che permettono al singolo di informarsi ed essere informato, dunque si dovrebbe avere una coscienza civile e politica più consapevole[206]. È necessario, però, un caveat. Anche se Internet e i social sono veicoli di informazione grazie ai quali ognuno può essere a conoscenza della corrente situazione politica interna ed estera, vi è il pericolo di imbattersi nelle notizie false o nella mera distorsione dei fatti, per cui ciò che è riportato non corrisponde alla realtà. Internet, infatti, è una fonte inesauribile di conoscenza che ha permesso a chiunque di produrre informazioni comportando anche ad un abbassamento della qualità dell'informazione stessa[207]. A seguito di questo generale impoverimento, dunque, si comprende il cortocircuito presente nell'isegoria. Poiché Internet e i social possono essere paragonati ad una moderna agorà in cui tutti possono esprimere la propria opinione risulta difficile, in realtà, avere un dialogo costruttivo che permetta uno scambio di opinioni. La vera natura della democrazia, infatti, consiste in un continuo confronto in cui vengono discusse diverse posizioni per giungere alla decisione che risulta essere la più *giusta* per tutti. Nelle democrazie di oggi questo aspetto pare essere passato in secondo piano, in quanto non sempre i governanti perseguono gli interessi dei governati. Questo fenomeno viene definito come post – democrazia, espressione coniata dal sociologo Colin Crouch. Per post – democrazia si intende la fase di declino che segue i periodi di democrazia forte, ovvero periodi in cui "*la gran parte dei gruppi e dei ceti identificabili tra i cittadini si organizzano autonomamente*

da tre avvocati iscritti all'albo speciale dei patrocinanti dinanzi alle magistrature superiori, oltre i componenti supplenti. Per ulteriori dettagli si veda https://www.giustizia.it/giustizia/it/mg_1_8_1.page?contentId=SDC467378

[205] Collina che nell'antichità era sede dell'*ecclesia.*

[206] Frosini,2017

[207] Montaldo, 2019

e attivamente nella vita politica"[208], nel quale rimangono le istituzioni democratiche, ma vengono guidate dalle grandi lobby[209]. L'uomo contemporaneo, dunque, non sta vivendo nella democrazia rappresentativa vera e propria, ma nell'era della post – democrazia.

In conclusione, non è semplice dare una definizione di democrazia, in quanto tale concetto assume significato diverso a seconda del periodo storico considerato. È evidente che tale mutamento derivi dai cambiamenti politici, economici e sociali per cui vi è una sensibilità diversa circa l'attuale forma di governo. Ciò che è certo, dunque, è la presenza di una varietà di forme di governo democratiche, ciascuna con le proprie peculiarità ed il recepimento dei principi fondamentali che hanno sorretto la democrazia ateniese per quasi tre secoli.

2. Dalla partecipazione elettorale…

Il concetto odierno di democrazia presenta una varietà di sfumature tutte diverse tra loro.

All'interno di questa varietà si può aprire una riflessione su due elementi espressivi della democrazia, ossia la partecipazione elettorale e la tutela dei diritti fondamentali. La ragione per cui si considerano questi elementi consta nel fatto che sono il risultato delle rivoluzioni a cavallo tra il Settecento e l'Ottocento che hanno segnato il passaggio da regimi monarchici assolutisti a forme di governo democratiche con la consolidazione del liberalismo. Successivamente a seguito della prima guerra mondiale vi è la formazione dei partiti di massa, affinché venissero ascoltate e rappresentate nei Parlamenti di tutta Europa le voci delle classi più deboli o comunque delle classi che hanno maggiormente sopportato il peso del primo conflitto mondiale. Se nell'Ottocento si era affermata la supremazia dell'uomo bianco borghese e proprietario terriero, nel primo periodo post-bellico, invece, anche l'uomo medio, analfabeta o che non fosse proprietario terriero e borghese aveva la possibilità di prendere parte alla vita politica. Il concetto stesso di partecipazione politica ha una pluralità di definizioni che ne impediscono una interpretazione univoca. Si può dare, dunque, una nozione ristretta che si traduce nell'esercizio del diritto al voto, nelle leggi elettorali e nel suffragio. In generale, dunque, se considerata in senso stretto la partecipazione elettorale concerne tutto ciò che riguarda l'elettorato e il suffragio. Vi è anche una nozione più ampia, ossia per partecipazione elettorale si intente "*ogni azione che direttamente o indirettamente miri a proteggere determinati interessi o valori o sia diretta a mutare o conservare gli equilibri nei rapporti sociali"*[210]. In tal senso, dunque, la partecipazione elettorale non è confinata al mero esercizio del diritto al voto, ma riguarda un qualsiasi comportamento del cittadino all'interno della società che ha come obiettivo il mantenimento o il sovvertimento degli

[208] Crouch, 2004
[209] *Ibidem*
[210] Enciclopedia Treccani, voce partecipazione elettorale.

equilibri sociali. Per quanto riguarda lo studio del tema della partecipazione elettorale si considera la nozione ristretta, in quanto strettamente correlata al tema del suffragio. La conquista del suffragio universale maschile e femminile è frutto di un lungo processo di cambiamenti economici, politici e dei costumi della società. In Italia il tema del suffragio è presente fin dalla concessione nel 1848 da parte di Re Carlo Alberto di Savoia dello Statuto albertino. È una prima forma di Costituzione, anche se all'epoca non venne chiamata così, poiché risultava eccessivo parlare di una carta fondamentale che sancisse i diritti e i doveri dei cittadini. Statuto, invece, è più moderato, in quanto dà l'idea che sia un qualcosa concesso dal monarca. Nello Statuto albertino non sono presenti molte disposizioni in materia di voto e suffragio, in quanto il tutto viene rimesso alla legge. È ben chiaro, però, chi sia detentore del potere, ossia il Re. All'articolo 5, ad esempio, viene sancito che *"Al Re solo appartiene il potere esecutivo"* e all'articolo 6 "*Il Re nomina a tutte le cariche dello Stato; e fa i decreti e regolamenti necessari per l'esecuzione delle leggi".* Inoltre, il Re è titolare del potere legislativo come affermato dall'articolo 7 dello Statuto[211]. Il cuore pulsante circa il tema della partecipazione elettorale è rappresentato dall'articolo 24, il quale apre la parte dedicata ai diritti e ai doveri dei cittadini e afferma "*Tutti i regnicoli, qualunque sia il loro titolo o grado, sono eguali dinanzi alla legge. Tutti godono egualmente i diritti civili e politici, e sono ammissibili alle cariche civili, e militari, salve le eccezioni determinate dalle Leggi".* In questo unico comma vengono sanciti alcuni principi che vale la pena evidenziare. Viene enunciato il principio di uguaglianza formale, ossia uguaglianza davanti alla legge. Tale principio, poi, viene recepito dall'art.3 co.1 della Costituzione il quale statuisce "*Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali".* È evidente che la presente disposizione sia molto più articolata nell'affermare l'uguaglianza formale tra cittadini rispetto al disposto dello Statuto albertino. *Tutti,* poi*, godono di diritti civili e politici.* Il termine *tutti* è neutro, dunque la naturale conclusione è che anche le donne avessero la possibilità di esercitare il diritto al voto e di essere elette, ossia di far parte dell'elettorato passivo. Così, invece, non è. Se si osservano le leggi elettorali che si sono susseguite, a partire dalla legge n.689/1848 promulgata da Re Carlo Alberto, si evince un suffragio piuttosto limitato. Vi era la volontà e anche, forse, la necessità di tenere separate la sfera politica da quella familiare ed evitare che si influenzassero a vicenda. Durante il Regno solo gli uomini di età non inferiore a venticinque anni che fossero in grado di leggere e scrivere e che pagassero un censo di quaranta lire[212] potevano votare. Successivamente, con la legge n.999/1882 vi è un primo ampliamento del suffragio maschile che venne esteso a tutti i cittadini maggiorenni che

[211] Articolo 7 Statuto albertino: *"Il Re solo sanziona le leggi e le promulga".*
[212] Tratto da https://legislature.camera.it/cost_reg_funz/667/1157/859/documentotesto.asp

avessero superato l'esame del corso elementare obbligatorio o che, in alternativa, pagassero un contributo annuo pari a 19,80 lire[213]. Il suffragio universale maschile fu introdotto con la legge n.666/1912. L'età per votare aumenta, in quanto si passa dai venticinque anni ai trent'anni in assenza di requisiti di censo o di istruzione. Mentre per i maggiorenni che non avessero compiuto trent'anni permanevano le condizioni di censo e della prestazione del servizio militare o il possesso di titoli di studio. Anche in questo caso vi è un'alternativa che ha avuto come risultato, secondo le stime dell'epoca, un notevole allargamento del corpo elettorale passando da 3.300.000 a 8.443.205 elettori[214]. Il suffragio universale maschile vero e proprio è stato sancito con la legge n.1895 del 1918 che lo ha esteso a tutti i cittadini che avessero compiuto ventun anni e, prescindendo dai limiti d'età, a tutti coloro che avessero prestato servizio nell'esercito mobilitato. Si voleva, dunque, premiare lo sforzo bellico e consentire a tutti i regnicoli di sesso maschile a votare registrando, dunque, un progressivo allargamento del suffragio. Si è passati da un suffragio ristretto che permetteva l'esercizio del diritto al voto all'uomo borghese e proprietario terriero che si stava affermando a inizio del XIX secolo ad un suffragio più ampio consentendo a tutti i cittadini maschi[215] indistintamente di votare nel primo post-guerra. Questo è anche il periodo in cui nascono e si consolidano i partiti di massa che intendono supportare le voci di chi ha combattuto e ha vissuto l'orrore sulla sua pelle. Partiti che garantiscono un pluralismo che verrà meno a pochi anni di distanza con l'ascesa della dittatura fascista. In tutto ciò le donne vengono escluse. Tale esclusione viene formalizzata con la legge n.2248 del 1865 Allegato A sull'unificazione amministrativa del Regno che statuisce all'articolo 26 "*Non sono né elettori, né eleggibili […] le donne"*[216]. La donna veniva esclusa tout court dalla vita politica ed economica del Regno. Le ragioni di tale esclusione sono fondate principalmente sulla posizione e sul ruolo che la donna occupava consistente principalmente nella cura e nell'educazione agli affetti. Si riteneva che le donne non fossero in grado di sviluppare una propria opinione sulle questioni politiche che non fossero influenzate da quella dei loro padri e dei loro mariti e, dunque, risultavano prive di una intelligenza politica[217]. È un'argomentazione a sostegno dell'esclusione dal diritto al voto che si fonda sull'inferiorità morale e intellettuale del *gentil sesso* legato al focolare domestico e per tal

[213] *Ibidem*
[214] *Ibidem*
[215] Per semplicità si parla di cittadini, in realtà non è una dicitura del tutto corretta, in quanto era ancora presente la monarchia.
[216] Il testo per intero dell'art.26 della legge n.2248/1865 recita *"Non sono né elettori, né eleggibili gli analfabeti, quando resti nel comune un numero di elettori doppio di quello dei consiglieri; le donne, gli interdetti, o provvisti di consulente giudiziario; coloro che sono in istato di fallimento dichiarato, o che abbiano fatto cessione di beni, finché non abbiano pagati intieramente i creditori; quelli che furono condannati a pene criminali, se non ottennero la riabilitazione; i condannati a pene correzionali od a particolari interdizioni, mentre le scontano; finalmente i condannati per furto, frode o attentato ai costumi"*.
[217] Isastia, 2008

ragione non poteva occuparsi anche di politica. Vi sono, poi, motivi di natura consuetudinaria, ossia le donne non hanno mai votato quindi non ci sarebbe alcuna ragione per conferire tale diritto. Inoltre, la politica in sé è competizione, scontro e votare significa prendere una posizione, schierarsi e ciò, all'epoca, era considerato inopportuno[218]. Una delle maggiori emancipazioniste italiane, ossia Anna Maria Mozzoni considerava il voto come elemento indispensabile per raggiungere la parità tra i sessi. È stata la prima donna in Italia a presentare una petizione per i diritti civili politici femminili richiedendo l'ammissione del sesso debole al voto amministrativo. In particolare, la Mozzoni dimostra come siano presenti delle contraddizioni tra il Codice civile e il Codice penale. Per il Codice civile del 1865 la donna è priva della capacità giuridica, mentre per il Codice penale Zanardelli del 1889 è imputabile e dunque penalmente perseguibile[219]. Il Codice civile, infatti, all'art.1106, ad esempio, prevedeva tra le categorie di esclusi a contrarre *le donne maritate*[220]. Il fatto che la donna sposata non potesse contrarre implica l'impossibilità di essere titolare diritti e doveri giuridici e quindi di avere capacità giuridica. Per il Codice Zanardelli, invece, la donna è penalmente perseguibile. Ad esempio, l'art.381 puniva l'aborto statuendo *"La donna che, con qualunque mezzo, adoperato da lei, o da altri col suo consenso, si procura l'aborto è punita con la detenzione da uno a quattro anni"*[221]. Ulteriore esempio di come la donna fosse ritenuta imputabile nel Codice penale del 1889 è il reato di adulterio punito dall'art.353[222]. Questi sono solo alcuni esempi dell'imputabilità della donna che implicano capacità giuridica[223]. La donna, dunque, nella percezione dell'epoca non era in grado di autodeterminarsi e di essere *libera*, ma era, invece, incatenata al suo ruolo di custode del focolare domestico rimanendo, quindi, a lungo esclusa dalla vita politica e lavorativa, soprattutto in ambito giuridico. Solo nel primo dopoguerra si iniziò a riflettere sul ruolo della donna nel mondo del lavoro giungendo ad un'apertura in tal senso con la legge n.1179/1919, la quale all'articolo 7 statuì l'ammissione delle donne – al pari degli uomini – ad esercitare tutte le professioni e a ricoprire tutti gli impieghi pubblici, tranne quelli che implicano "*poteri giurisdizionali o l'esercizio di potestà politiche, o che attengono alla difesa militare dello Stato […]"*[224].La legge Sacchi, ossia la legge n.1179/1919, nonostante abbia posto il divieto di accesso alle donne alle professioni che implicano l'esercizio dei poteri giurisdizionali come, ad esempio, la professione forense o la magistratura, è stata rivoluzionaria poiché ha sancito l'abolizione dell'istituto dell'autorizzazione maritale previsto

[218] *Ibidem*
[219] *Ibidem*
[220] Codice civile 1865
[221] Codice penale 1889
[222] Art.353 Codice penale, 1889: "*La moglie adultera è punita con la detenzione da tre a trenta mesi".*
[223] Si noti come sono reati attinenti alla sua sfera sessuale e come siano strettamente correlati al suo ruolo di madre e moglie.
[224] Art.7 l.1179/1919

all'art.134 del Codice Civile del 1865[225] prevedendo l'emancipazione giuridica della donna, in quanto prima del 1919 ella non poteva compiere una serie di atti che implicavano necessariamente il suo prendere parte alla vita economica e lavorativa all'interno del tessuto sociale, se non in presenza dell'autorizzazione del marito. È ragionevole ritenere che alla donna fosse preclusa la possibilità di esercitare tali atti, in quanto ancora priva della possibilità di esercitare il diritto politico più rilevante tra tutti, ossia il diritto al voto. Se non poteva partecipare alla vita politica del Regno, non poteva pertanto partecipare alla sua vita economica mettendo ancora di più, quindi, in risalto il suo ruolo di colei che si prende cura della casa e della famiglia. Nel corso del tempo vi furono delle accese discussioni circa il ruolo della donna, soprattutto in riferimento alla sua ammissibilità o meno all'esercizio della professione forense e della magistratura. Ad esempio, durante la discussione circa l'ammissibilità o meno delle donne all'accesso agli impieghi pubblici e privati[226] nella seduta del 20 settembre 1946 dell'Assemblea costituente l'onorevole Enrico Molè sollevò qualche dubbio circa la parificazione dei sessi in tutti gli uffici, in quanto *"tale parificazione non è possibile, ad esempio, in quelli [uffici] che riguardano le funzioni giudiziarie e militari"*[227]. Affermazione giustificata sia da argomenti di diritto, in quanto già nel diritto romano era stato riconosciuto che la donna in alcuni periodi della sua vita non ha la piena capacità di lavoro sia da argomenti di carattere scientifico, poiché "*da studi specifici sulla funzione intellettuale in rapporto alle necessità fisiologiche dell'uomo e della donna risultano certe diversità, specialmente in determinati periodi della vita femminile"*[228]. Si tratta di argomenti che sono figli del proprio tempo e sostenuti fin dalla fine del XIX secolo con il cc.dd. caso Poet[229] per cui alle donne veniva interdetto l'accesso ai pubblici uffici non tanto per ragioni

---

[225] Il quale recita(va): "*La moglie non può donare, alienare beni immobili, sottoporli ad ipoteca, contrarre mutui o riscuotere capitali, costituirsi sicurtà, né transigere o stare in giudizio relativamente a tali atti, senza l'autorizzazione del marito. Il marito può con atto pubblico dare alla moglie l'autorizzazione in genere per tutti o per alcuni di detti atti, salvo a lui il diritto di rivocarla".*

[226] Il testo dell'articolo proposto e discusso era il seguente: "*Tutti i cittadini italiani, senza distinzione di sesso sono ammessi agli impieghi pubblici in base ai concorsi, senza alcuna restrizione, tranne quella della capacità. L'esercizio dell'insegnamento universitario è aperto a tutti i capaci indipendentemente da distinzioni di razza, religione, credo politico e nazionalità. L'accesso agli impieghi privati e aperto a tutti i cittadini italiani senza distinzione di sesso".*

[227] Tratto dal resoconto sommario della seduta dell'Assemblea costituente del 20 settembre 1946. Si veda http://legislature.camera.it/_dati/costituente/lavori/iii_sottocommissione/sed009/sed009nc.pdf#page=4&zoom=95,0,70

[228] *Ibidem*

[229] Lidia Poet, laureatasi in giurisprudenza nel 1881, dopo il biennio di pratica forense richiede e ottiene l'iscrizione all'albo degli avvocati di Torino a seguito di una decisione approvata dalla maggioranza dal Consiglio dell'ordine di Torino. La sua iscrizione fu immediatamente impugnata davanti alla Corte d'Appello di Torino dalla procura generale. La Corte d'Appello decide in senso negativo, perciò alla Dottoressa Poet fu radiata dall'albo. Le ragioni su cui si fonda la decisione della Corte d'Appello, ragioni che poi verranno anche confermate in Cassazione nel 1884, non sono tanto di diritto ma attengono, invece, alla natura del *gentil sesso* e alla sua indole. In Cassazione, oltre a presentare delle argomentazioni basate sulla natura della donna, si presta attenzione anche all'interpretazione della legge sulla professione forense, ossia la legge dell'8 giugno 1874 n.1938 rilevando come *" [la legge] non ha pensato di attribuire alle donne l'esercizio delle funzioni sociali di ragion pubblica e per il motivo […] in tutti gli atti preparatorii, sia governativi, sia parlamentari di quella legge, non è fatta menzione di alcun diritto delle donne"* e ancora "*è troppo ardita la pretesa di voler trovare in una legge sulla pubblica istruzione una dichiarazione generale nel senso, che il diploma ottenuto da una donna basti per far nascere la capacità relativa e la condizione di diritto all'esercizio della professione di avvocato".* Per ulteriori dettagli si veda Corte di

giuridiche, ma per ragioni di mero fatto che spaziano dallo strano effetto che avrebbe avuto la toga indossata sopra gli abiti femminili all'allusione alla bellezza femminile che fungerebbe da distrazione in quanto i giudici avrebbero perso quella lucidità necessaria per esercitare il loro magistero davanti ad un'*avvocatessa attraente*[230]. Solo nel 1963 vi è stata un'apertura alle donne in riferimento alla vita politica e giuridica con la legge n.66/1963 composta da soli due articoli. L'art.1 co.1 statuisce che "*La donna può accedere a tutte le cariche, professioni e impieghi pubblici, compresa la Magistratura, nei vari ruoli […] senza limitazione di mansioni e di svolgimento di carriera, salvi i requisiti stabilii dalla legge."*[231] ponendo, dunque, un punto fermo alle discussioni circa l'ammissibilità o meno delle donne all'esercizio della professione forense e di magistrato. Tornando al punto, ossia il suffragio, è interessante osservare come malgrado si ritenesse che donne non potessero votare, la Corte d'Appello di Ancona fu la prima ad ammettere l'iscrizione delle donne alle liste elettorali politiche in quanto conforme allo Statuto albertino[232]. Venne data un'interpretazione dell'articolo 24 inclusiva, per cui la disposizione in questione ricomprendeva anche le donne in quanto l'espressione *tutti i regnicoli* abbraccia sia il sesso maschile sia quello femminile essendo un'espressione neutra. Inoltre, a rafforzare la posizione della Corte si considera l'articolo 25 dello Statuto, il quale prevede l'obbligo di contribuzione al Regno in proporzione agli averi includendo anche le donne, in quanto non vi è dubbio che anch'esse al pari degli uomini fossero contribuenti in proporzione ai loro averi[233]. Andando in avanti con la linea del tempo, con il regime fascista si avrà un'apertura al suffragio universale. Nel 1923, infatti, fu presentato alla Camera un disegno di legge per il voto amministrativo limitato. Solo le donne che avessero compiuto venticinque anni, decorate per meriti di guerra o che fossero madri di caduti di guerra, che avessero concluso le scuole dell'obbligo e che pagassero le tasse erano ammesse al voto. Si tratta di criteri piuttosto stringenti che andavano a limitare l'elettorato femminile, ma è un primo spiraglio di apertura al suffragio. È uno spiraglio proprio perché nel 1926 vennero, poi, abolite tutte le forme di elezione delle amministrazioni comunali[234] e dunque le donne furono nuovamente private del diritto al voto. Solo in seguito alla caduta del fascismo, nel 1945 venne emanato un decreto che approvava il voto alle donne. Come è noto, il 2 giugno del 1946 le donne votarono per la prima volta in un referendum istituzionale per decidere quale forma di governo adottare se la monarchia o la repubblica. È interessante osservare come il primo voto che venne espresso dal cc.dd. sesso debole fu su un referendum e non nell'ambito di una elezione politica, ma, nonostante ciò, venne data per la

Cassazione di Torino, udienza 18 aprile 1884 tratta da https://www.penaledp.it/wp-content/uploads/2023/02/decisione-della-Suprema-Corte-di-Cassazione-di-Torino.pdf
230 Mazzucca, 2023
231 Art.1 legge n.66/1963
232 Isastia, 2008
233 *Ibidem*
234 *Ibidem*

prima volta la possibilità di prendere posizione e di far valere la propria voce. Ad oggi, grazie all'art.48 della Costituzione viene garantito il suffragio universale con dei limiti, sanciti all'ultimo comma, all'esercizio del diritto al voto per "*incapacità civile o per effetto di sentenza penale irrevocabile o nei casi di indegnità morale indicati dalla legge".* Tali sono le ipotesi tassativamente previste dalla Costituzione che ostano il diritto al voto, oltre all'essere privi della cittadinanza italiana e il non aver ancora raggiunto la maggior età. Altre condizioni o limitazioni non sono presenti, dunque, è chiaro l'intento del Costituente: l'assenza di alcuni criteri o, meglio, discriminazioni come il sesso o il censo è funzionale al coinvolgimento di più persone possibili alla vita politica del Paese chiamate a prendere una decisione ed eleggere i loro rappresentanti in Parlamento. Inoltre, il suffragio universale è indice di democraticità del Paese, per cui ogni cittadino è chiamato ad esercitare tale diritto, ma prima di tutto dovere civico. Si vuole evitare, dunque, di rivivere l'esperienza della dittatura fascista e permettere a ogni cittadino di esprimersi liberamente.

3. … alla tutela dei diritti fondamentali

Il concetto di democrazia, come si è visto in precedenza, è molto ampio per cui cercare di darne una definizione univoca è un'operazione alquanto complessa. Si è osservato, infatti, come democrazia ad oggi sia un termine ricco di sfumature che vanno dalla nozione *classica,* ossia si fa riferimento alla democrazia rappresentativa alla nozione più *moderna* con la cc.dd. democrazia elettronica. Nonostante la difficoltà nel dare una definizione che esprima in modo chiaro che cosa significhi democrazia, sono stati individuati due elementi chiave comuni alle diverse forme di governo democratico ossia la partecipazione elettorale e la tutela dei diritti fondamentali. Si è analizzato nel paragrafo precedente che cosa voglia dire partecipazione elettorale, ma si evince come ciò non sia sufficiente affinché si possa parlare di democrazia. Il cuore pulsante della democrazia risiede nel dialogo a più voci, ossia da un lato la maggioranza, dall'altro la minoranza affinché si possa giungere alla *miglior scelta* che soddisfi gli interessi dei governati. Detto così sembrerebbe che ciò sia già ampiamente garantito dalla possibilità per i cittadini di esercitare il diritto al voto eleggendo i loro rappresentanti in Parlamento, i quali formando la maggioranza di governo risultano essere i portatori degli interessi dei governati e dunque la tutela dei diritti fondamentali risulterebbe essere superflua. In realtà, al fine del corretto funzionamento dell'intero apparato democratico è necessaria la tutela dei diritti cc.dd. fondamentali, come i diritti civili, politici e sociali, poiché in difetto non sarebbe in un regime democratico, ma autoritario. La tutela di certi diritti fondamentali, come il diritto al voto, il diritto di manifestare liberamente il proprio pensiero ma anche la tutela dell'individuo come singolo e nelle formazioni sociali consente, dunque, una partecipazione attiva del cittadino alla vita politica, sociale ed economica del Paese, oltre a garantire il cc.dd. Stato di diritto elemento cardine sia dell'ordinamento nazionale

sia dell'ordinamento sovranazionale[235]. Per Stato di diritto generalmente si intende la presenza di un corpus di norme regolatrici l'attività degli organi statuali e il loro rapporto con i privati e i cittadini. In sostanza, nello Stato di diritto sono presenti norme giuridiche generali e astratte che hanno lo scopo di controllare e limitare il potere statuale[236] evidenziando, così, il netto contrasto con lo Stato assoluto nel quale, invece, il potere statuale è concentrato nelle mani di un unico soggetto. Si comprende, dunque, come la tutela dei diritti fondamentali sia necessaria affinché si possa disquisire di democrazia ed è altrettanto evidente, come verrà illustrato nel proseguo della trattazione, che l'attenzione su tale tematica è emersa in tempi relativamente recenti, ossia nel secondo dopoguerra periodo di rinascita degli apparati giuridici e statuali Europei. Per quanto attiene alla nozione di diritti fondamentali, si potrebbe affermare che essi sono diritti umani che appartengono all'uomo in quanto tale funzionali ad assicurarne la dignità, la libertà e il benessere sociale senza alcuna discriminazione basata sulla nazionalità, sesso, etnia, religione, lingua o altri fattori che potrebbero essere considerati discriminanti[237]. Per tale ragione, dunque, i diritti fondamentali sono universali, inalienabili e interdipendenti. Universali, in quanto spettano a chiunque. Inalienabili, poiché non possono essere perduti o limitati se non in casi specificamente previsti[238]. Infine, sono interdipendenti in quanto sono intrinsecamente connessi l'uno all'altro[239], ad esempio non vi può essere un libero esercizio del diritto al voto se non vi è la possibilità di essere informati e di informarsi liberamente.

[235] A livello Europeo si fa riferimento all'art.2 del TUE il quale statuisce "*L'unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini".* Per quanto riguarda lo Stato di diritto, affinché esso venga rispettato da tutti gli Stati membri sono previsti alcuni strumenti a suo presidio come dialoghi annuali in sede di Consiglio Affari Generali e lo strumento maggiormente conosciuto, ossia il meccanismo previsto dall'art.7 TUE in caso di violazioni del dispositivo dell'art.2 TUE che non siano *una tantum,* ma sistematiche. Per quanto riguarda la procedura ex art.7 TUE, prima di constatare l'effettiva violazione dei valori previsti dall'art.2 TUE viene data la possibilità allo Stato membro in questione di esporre le proprie ragioni con la possibilità da parte del Consiglio di rivolgergli delle raccomandazioni. Le maggioranza previste affinché tale procedura possa essere messa in auge sono particolarmente elevate. A titolo di esempio, solo per dare avvio a tale meccanismo è necessario che vi sia la proposta motivata di un terzo degli Stati membri, del Parlamento Europeo o della Commissione Europea e il Consiglio delibera con la maggioranza dei quattro quinti dei sui membri constatando il mero rischio di una violazione grave dell'art.2 TUE da parte di uno Stato membro, mentre per quanto riguarda la constatazione di una violazione grave dell'art.2 TUE il consiglio delibera all'unanimità su proposta di un terzo degli Stati membri o della Commissione previa approvazione del Parlamento europeo. Visti I quorum necessari per l'attivazione dell'intera procedura è chiaro come essa non trova particolare applicazione, per cui la tutela risulta essere alquanto farraginosa.

[236] Enciclopedia Treccani, voce Stato di diritto.

[237] United Nations, definizione di diritti umani.

[238] *Ibidem*

[239] *Ibidem*

3.1. La nascita dei diritti fondamentali

Se si guarda alla storia di diritti fondamentali, in un certo senso, se ne parlava già nel Medioevo, in seguito di alcune concessioni rese dal sovrano affinché si raggiungesse un accordo tra il potere regnante e la nobilità. Un esempio è la Magna Charta Libertatum, concessa da Re Giovanni d'Inghilterra nel 1215, un documento di sessantatré articoli accogliente le richieste baronali. Per l'epoca la Magna Charta fu rivoluzionaria, poiché per la prima volta un sovrano riconosceva la libertà e l'inviolabilità della Chiesa, come affermato dall'articolo 1 " *[…] la Chiesa d'Inghilterra sarà per sempre libera e i suoi diritti non saranno ridotti e le sue libertà non saranno violate"*[240] e dei cittadini statuendo "*A tutti gli uomini liberi del Nostro Regno abbiamo inoltre garantito […] tutte le libertà scritte in questa carta"*[241] e le prerogative del ceto baronale. Inoltre, l'elemento di novità della Magna Charta risiede nel fatto che il sovrano sembra fare *un passo indietro* rispetto al proprio potere, in quanto agisce solo in presenza del consenso dei sudditi o si astiene dal compiere determinate azioni[242]. Facendo un salto temporale in avanti, nel XVIII secolo un'altra pietra miliare per lo sviluppo dei diritti fondamentali è la Dichiarazione Universale dei diritti dell'uomo e del cittadino del 1789 che fu il preambolo della Costituzione francese del 1791 e il propulsore per le successive costituzioni del 1793 e 1795. Nella parte introduttiva viene sancita la necessità di dichiarare diritti *naturali, inalienabili e sacri dell'uomo* affinché vengano stabiliti, da un lato i diritti e i doveri dei cittadini e dall'altro la separazione tra il potere legislativo e quello esecutivo[243]. Spostandosi in territorio italiano una cinquantina di anni dopo, nel 1848, venne concesso lo Statuto albertino sancendo a partire dall'art.24 i diritti e i doveri dei cittadini[244]. Si registra, dunque, con il passare dei secoli un progressivo ampliamento delle libertà e dei diritti dell'uomo e del cittadino. Il punto di svolta è tra il XIX e il XX secolo periodo in cui vi è il passaggio dall'ordinamento liberale a quello costituzionale. Nel XIX secolo i diritti esistevano in quanto previsti dalla legge. All'epoca non erano ancora presenti le Costituzioni come conosciute nei giorni nostri, per cui la legge era la fonte suprema e illimitata del diritto[245]. Essendo previsti dalla legge, caratterizzata dalla generalità ed astrattezza[246], i diritti e le libertà che si intendevano tutelare mutavano con il passare del tempo a seconda dei valori considerati e del contesto

[240] Magna Charta, 1215
[241] *Ibidem*
[242] Ad esempio all'articolo 31 della Magna Charta si afferma *"Né noi né alcun ufficiale reale prenderemo legna per il Nostro castello o per Nostra necessità, se non con il consenso del proprietario del bosco".*
[243]https://scienzepolitiche.unical.it/bacheca/archivio/materiale/143/Storia%20contemporanea/Dichiarazione%20diritti%20uomo%20e%20cittadino%201789.pdf
[244] A titolo di esempio, nell'articolo 25 veniva sancito il dovere di contribuzione alle spese del regno in base ai propri averi. Negli articoli 27 e 29 veniva sancita l'inviolabilità del domicilio e della proprietà che poteva venir meno in casi eccezionali.
[245] Ferrajoli, 2014
[246] Per generalità si intende la capacità della norma di regolare fatti o comportamenti senza fare riferimento a situazioni o soggetti determinati. Per astrattezza si intende la ripetibilità della regola per un tempo indeterminato. Si veda Pisaneschi, 2018,

di riferimento. Ciò comporta ad un indebolimento nella tutela dei diritti e delle libertà, indebolimento che viene rafforzato anche dal principio *lex posterior abrogat priori* in virtù del quale la legge successiva abroga la legge precedentemente adottata. Ne è un esempio lo Statuto albertino che dal punto di vista formale è una Costituzione ottriata[247] e flessibile, dunque facilmente modificabile con l'adozione di leggi ordinarie che ne mutano o integrano il contenuto. Con la promulgazione tra il 1925 e il 1926 delle leggi fascistissime, le quali avevano incrementato le prerogative e il potere dell'Esecutivo a discapito del potere sovrano, si è messo in atto tale principio per cui lo Statuto albertino, di fatto, è stato *abrogato* e privato di valore giuridico. Il passaggio da testi costituzionali brevi[248] e flessibili a Costituzioni lunghe e rigide lo si ha con il secondo dopoguerra. A seguito dell'esperienza della seconda guerra mondiale e dei regimi dittatoriali vi era la necessità di promulgare testi costituzionali dotati di queste caratteristiche a presidio della nuova forma di governo adottata, ossia la democrazia. La democrazia viene tutelata, dunque, con una Costituzione lunga, ossia che descrive in modo preciso e approfondito il funzionamento degli organi statuali e le libertà e diritti fondamentali garantiti e, dunque, in quanto costituzionalmente protetti inviolabili. Per evitare un ritorno al passato, la Costituzione post 1945 è rigida, ossia non è possibile modificarla o integrarla se non con un procedimento aggravato. Come afferma Luigi Ferrajoli, la rigidità della Costituzione è fondamentale, in quanto serve per "*legare le mani delle generazioni future per impedire che taluna di queste possa amputare le mani alle generazioni successive"*[249]. Detto altrimenti, impedire che il testo costituzionale venga modificato con una legge ordinaria tutela la Costituzione stessa e serve a rafforzare la democrazia impedendo possibili derive autoritarie o dittatoriali. Il secondo dopoguerra, dunque, è stato essenziale per la conformazione e consolidazione dei diritti fondamentali come conosciuti oggi. Il mondo intero stava cercando di risorgere dalle ceneri della guerra e di ricostruirsi anche dal punto di vista dell'assetto istituzionale, politico ed economico.

3.2. I diritti fondamentali nel quadro internazionale

Nel contesto delle nuove Costituzioni dotate delle caratteristiche di essere rigide e lunghe[250] si inserisce anche il tema dei diritti fondamentali e del loro ampliamento e sviluppo a partire dalla Dichiarazione Universale dei diritti dell'uomo del 1948 emanata dall'ONU e dalla Convenzione Europea dei diritti

[247] Per Costituzione ottriata si intende una Costituzione concessa dal sovrano.
[248] Per Costituzione breve si intende un testo descrive in generale l'assetto organizzativo dello Stato prevedendo qualche diritto e libertà fondamentali.
[249] Ferrajoli, 2014
[250] Per costituzione lunga si intende un testo composto da un elevato numero di articoli che descrive in modo chiaro e preciso i diritti fondamentali dei cittadini, ma anche l'assetto organizzativo dello Stato, nonché i rapporti sociali ed economici.

dell'uomo[251] firmata nel 1950 dagli Stati membri del Consiglio d'Europa. Essendo due documenti coevi è possibile fare un breve confronto fra essi. È immediatamente evidente come i diritti prescritti dalla Dichiarazione del 1948 siano effettivamente dotati della caratteristica dell'universalità, in quanto l'articolo 1 statuisce le condizioni di libertà ed eguaglianza in dignità e diritti spettanti a tutti gli esseri umani[252]. La dignità è particolarmente rilevante, in quanto è la base dei diritti fondamentali e senza di essa non si può trattare di tale tema essendo garante dell'universalità dei diritti umani. Dignità che viene riconosciuta anche dalla Costituzione italiana nella dimensione sociale, in riferimento all'articolo 3 co.1, il quale statuisce il principio di eguaglianza formale statuendo "*Tutti i cittadini hanno pari dignità sociale* [253]. Dignità sociale che viene, poi, ripresa dall'articolo 36 declinato in termini lavoristici affermando il diritto ad una giusta retribuzione che sia comunque sufficiente ad assicurare al lavoratore e alla sua famiglia *"un'esistenza libera e dignitosa"*[254]. Un ulteriore esempio della dimensione della dignità umana declinata nel tema della garanzia dei diritti fondamentali è dal punto di vista economico con l'articolo 41, il quale prevede la libertà di iniziativa economica privata che deve potersi svolgere senza recare danno alla dignità umana[255].

L'universalità dei diritti sanciti dalla Dichiarazione ONU del 1948, poi, è evidente nel secondo articolo, il quale sancisce la spettanza di tutti i diritti e le libertà enunciate nella dichiarazione senza alcuna distinzione. L'articolo, poi, procede ad una elencazione esauriente di alcuni fattori che potrebbero essere discriminanti e che impedirebbero un godimento universale delle libertà prescritte dalla Dichiarazione concludendosi con una clausola aperta, ossia " *[,,,] o di altra condizione"* [256] . La presenza di una clausola aperta è un chiaro segnale dell'impossibilità di considerare tutti i possibili fattori discriminanti che andrebbero ad annichilire il carattere universale dei diritti e libertà prescritte, in quanto ciò che in passato non era discriminatorio lo può essere nel presente. Inoltre, tale clausola contribuisce ad affermare e rafforzare il carattere universale dei diritti e delle libertà sancite dalla Dichiarazione. Per quanto riguarda la CEDU, invece, anche se l'intento è quello di tutelare diritti riconosciuti come fondamentali, essi non sono dotati della caratteristica dell'universalità, a differenza della Dichiarazione del 1948. Questo è evidente nel preambolo nel quale viene statuito l'intento del Consiglio d'Europa, ossia di *"realizzare un'unione più stretta tra i suoi membri"* e ciò è possibile attraverso la tutela e lo sviluppo dei diritti e libertà fondamentali dell'uomo[257]. Il fatto che il fine della

[251] Da ora in poi verrà abbreviata in CEDU.
[252] L'articolo 1 della Dichiarazione universale dei diritti dell'uomo del 1948 statuisce per la precisione "*Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti. Essi sono dotati di ragione e di coscienza e devono agire gli uni verso gli altri in spirito di fratellanza".*
[253] Art.3 co.1 Costituzione
[254] Art. 36 Costituzione
[255] Art.41 co.2 Costituzione
[256] Articolo 2 Dichiarazione Universale dei diritti dell'uomo.
[257] Consiglio d'Europa, 1950

CEDU sia quella di rafforzare l'unione tra gli Stati membri del Consiglio d'Europa è indicatore di una circoscrizione dei diritti fondamentali in una determinata area e per determinati soggetti. Bisogna osservare come la CEDU, nonostante i diritti e libertà previsti siano limitati solamente agli Stati membri del Consiglio d'Europa, sia stata fondamentale in quanto rappresenta un primo passo in avanti circa il riconoscimento dei diritti fondamentali in territorio europeo, poiché inizialmente il processo di integrazione europea era di carattere solo economico. L'obiettivo delle ex comunità europee, difatti, era la creazione di un mercato economico unico con lo scopo di risollevare l'economia europea alla fine della seconda guerra mondiale. I diritti e le libertà proclamate dalla Convezione del Consiglio d'Europa del 1950 trovano tutela giurisdizionale solo a partire dal 1959 con l'istituzione della Corte Europea dei diritti dell'uomo, ossia la Corte EDU. Un ulteriore punto di riferimento per lo sviluppo del tema dei diritti fondamentali è la Carta di Nizza, ossia la Carta dei diritti fondamentali dell'Unione Europea del 2000 la quale in base all'articolo 6 del TUE ha lo stesso valore giuridico dei Trattati[258]. La riflessione sui diritti fondamentali che ha portato alla stesura di tale documento è frutto del contesto sociopolitico degli anni '90 del secolo scorso, in particolare il genocidio in Rwanda del 1994 e la guerra del Kosovo tra il 1998 e il 1999. L'obiettivo della Carta di Nizza è quello di creare all'interno del territorio europeo uno spazio di libertà, sicurezza e giustizia rafforzando la tutela dei diritti fondamentali con particolare attenzione all'evoluzione della società e della tecnologia[259].

3.3. La tutela dei diritti fondamentali nell'ordinamento interno nei rapporti politici

Se dal punto di vista internazionale vi è prova di un certo interesse per questa tematica, dal punto di vista interno il faro che guida il legislatore nella definizione dei diritti fondamentali è la Costituzione, la quale riconosce e garantisce all'art.2 i diritti inviolabili dell'uomo sia come singolo sia nelle formazioni sociali. Sono diritti naturali, appartenenti all'uomo in quanto tale per cui l'ordinamento statuale si impegna a riconoscerli, garantirli e tutelarli. L'uomo viene considerato come individuo inserito nelle formazioni sociali che risultano essere essenziali per l'affermazione e lo sviluppo della sua personalità. A tal proposito si fa riferimento, ad esempio, alla famiglia, alla scuola, al lavoro e alla partecipazione alla vita politica del Paese. L'articolo 2 della Costituzione, dunque, si pone come fondamento di carattere giuridico per quanto riguarda l'individuazione dei diritti fondamentali. Ai fini della trattazione di tale tematica in Costituzione a presidio della democrazia si considera l'aspetto dei rapporti politici e in particolare il diritto al voto sancito all'articolo 48, la libertà di pensiero tutelata dall'articolo 21, la libertà di associazione prevista dall'articolo 18 della Costituzione. Sono

[258] La Carta di Nizza avendo lo stesso valore giuridico dei Tratti è parte delle fonti di rango primario dell'Unione Europea.
[259] Europarl, Carta di Nizza, 2001

disposizioni strettamente correlate tra loro, per cui risultano interdipendenti. Non vi può essere, infatti, un esercizio del diritto al voto consapevole se non vi è la possibilità di manifestare liberamente il proprio pensiero e di essere informati ed informarsi adeguatamente. Se non vi fosse, poi, la possibilità per i cittadini di associarsi non vi sarebbe l'opportunità di formare partiti politici, emblema del pluralismo democratico.

Il diritto al voto enunciato dall'articolo 48 è strettamente correlato con la tutela della democrazia, in quanto rappresenta la massima espressione della partecipazione dei cittadini alla vita politica del Paese chiamati ad eleggere ogni cinquennio i propri rappresentanti in Parlamento. L'esercizio del diritto al voto, dunque, è una delle forme con cui si manifesta la sovranità del popolo prevista dall'articolo 1 della Costituzione. Le elezioni sono cruciali per i parlamentari, poiché è in questo momento che il loro operato viene giudicato dagli elettori, i quali potranno rieleggere la maggioranza di Governo oppure affidare l'Esecutivo all'opposizione. Tramite il voto, dunque, i cittadini sono in grado di influenzare la politica del Paese. Il recarsi alle urne, inoltre, non è più un obbligo giuridico ma un dovere civico. Il d.lgs. n.534/1993 all'articolo 3 ha sancito, infatti, l'abrogazione dell'articolo 115 del D.P.R. n.361/1957 il quale prevedeva un elenco esposto nell'albo comunale dei nomi di coloro che si sono astenuti dal votare in assenza di un giustificato motivo e la menzione per un periodo di cinque anni "non ha votato" nei certificati di buona condotta. È evidente come l'esposizione del proprio nominativo in un elenco consultabile da chiunque e la menzione "non ha votato" nei certificati di buona condotta rilasciati a chi si è astenuto senza un giustificato motivo siano una sorta di gogna pubblica che espone l'elettore. Se da un lato la previsione di un obbligo giuridico di esercizio del diritto al voto con conseguente sanzione poteva essere un rimedio all'assenteismo, dall'altro bisogna forse ritenere che non fosse la soluzione migliore per contrastare tale fenomeno e ciò, dunque, ha portato all'eliminazione di tale obbligo. Il voto, quindi, è un diritto ma prima di tutto un dovere civico. È un dovere civico connotato dalle caratteristiche della personalità, uguaglianza, libertà e segretezza[260]. La personalità del voto sottintende il fatto che l'elettore deve recarsi personalmente alle urne e dunque vi è un divieto per il legislatore di introdurre regole che consentano il voto per delega, ossia l'elettore attribuisce l'esercizio del proprio diritto ad un altro soggetto autorizzato a votare facendo le veci del delegante. La personalità è essenziale, in quanto se fosse ammesso il voto per delega ciò comporterebbe a potenziali abusi, in quanto non vi è la certezza assoluta che il voto espresso dal soggetto delegato sia effettivamente corrispondente a quanto indicato dal delegante. Il voto, poi, è uguale, ossia viene rispettato il principio una testa un voto per cui non sono ammessi voti plurimi per determinate categorie di persone facendo sì che ogni voto abbia lo stesso peso. Il voto, poi, è libero,

[260] Articolo 48 co.2 Costituzione

ossia ogni cittadino deve essere in grado di esprimere la propria preferenza in assenza di coercizioni esterne che vadano ad influenzare e manipolare l'esercizio di tale diritto. Libertà che implica anche la possibilità per l'elettore di poter scegliere tra una rosa di candidati o di esprimere un voto nullo se nessuno dei candidati incontra le sue preferenze. Sulla libertà di scelta la celebre sentenza della Corte costituzionale n.1/2014, oltre a concentrarsi sul premio di maggioranza come previsto dalla legge elettorale 270/2005 pone l'attenzione sulle liste bloccate, le quali impedirebbero all'elettore di esprimere una preferenza sul candidato consentendogli solo di scegliere una lista di partito. La Corte ritiene fondata tale questione, poiché i voti espressi scegliendo solo la lista *"escludono ogni facoltà dell'elettore di incidere sull'elezione dei propri rappresentanti"* precisando che la scelta dell'elettore "*si traduce in un voto di preferenza esclusivamente per la lista […] rendendo difficilmente conoscibili [n.d.s. i candidati] dall'elettore stesso".*[261] La Corte, poi, rileva come la disciplina delle liste bloccate privi l'elettore di ogni scelta del proprio rappresentante politico rimettendola ai partiti. Con tale sistema, dunque, verrebbe meno la libertà di scelta dei candidati da parte dell'elettore violando conseguentemente l'articolo 48 co.2 della Costituzione. Ultima, ma non per importanza, la caratteristica della segretezza funzionale a tutelare la libertà dell'elettore, ossia si vogliono evitare coercizioni o condizionamenti sulla persona dell'elettore. Segretezza che non riguarda solo la tutela della libertà, in quanto si manifesta concretamente alle urne. La presenza, difatti, di una cabina elettorale, di pubblici ufficiali che procedono all'identificazione, la scheda elettorale e la matita compilativa sono strumenti a presidio della segretezza. Tale caratteristica, dunque, ha una dimensione personale strettamente correlata alla persona dell'elettore, ma anche una dimensione rituale. A livello giuridico la segretezza del voto è tutelata con il d.l. n.49/2008 convertito nella legge n.96/2008 che vieta l'introduzione all'interno delle cabile elettorali di cellullari o *"altre apparecchiature in grado di fotografare o registrare immagini"*[262]. Il Legislatore del 2008, dunque, era consapevole del possibile utilizzo da parte degli elettori di strumenti tecnologici che potenzialmente minerebbero la segretezza del voto sanzionando la trasgressione con l'arresto da tre a sei mesi e con l'ammenda da 300 a 1000 euro[263]. L'asprezza della sanzione, dunque, fa comprendere quanto la segretezza del voto sia rilevante e che necessiti di un'adeguata tutela. Segretezza, poi, che viene messa in discussione nei tempi più recenti a seguito del dibattito sull'implementazione del voto elettronico. Tale tema verrà affrontato nei prossimi capitoli, per ora è sufficiente osservare come la segretezza verrebbe meno nelle forme di voto elettronico non presidiato, ossia l'elettore esprime la propria preferenza tramite applicazioni o siti web

[261] Sentenza n.1/2014 Corte Costituzionale
[262] Articolo 1 d.l. n.49/2008
[263] *Ibidem*

in qualsiasi luogo e terminale in assenza di un supervisore o pubblico ufficiale[264]. Il problema della segretezza si pone, in quanto l'elettore potendo esprimere la propria preferenza da qualsiasi dispositivo e in qualsiasi luogo potrebbe essere soggetto a pressioni esterne che gli impedirebbero di esprimere genuinamente la sua preferenza.

Strettamente correlato con l'esercizio del diritto al voto, l'articolo 21 della Costituzione tutela la libertà di opinione, la quale rappresenta una delle conquiste più importanti a livello di diritti fondamentali soprattutto dopo l'esperienza del Ventennio. L'importanza di tale libertà è percepita anche a livello contenutistico. Si rileva, innanzitutto, come la libertà di manifestare il proprio pensiero sia tutelata tout court, in quanto la Costituzione considera a tal fine qualsiasi mezzo di diffusione come esplicitato al primo comma. Risaltano, poi, il terzo e il quarto comma, in quanto è presente una approfondita disciplina circa la stampa e i casi in cui è concesso procedere al sequestro. Sono evidenti le ragioni di carattere storico che hanno spinto i padri costituenti a porre in essere una disciplina di tal genere. È possibile, poi, effettuare un confronto tra l'articolo 21 e l'articolo 13 della Costituzione tutelante la libertà personale per quanto riguarda la modalità di restrizione previste. Se si osservano i due dettati normativi, per quanto concerne tal punto, il lessico utilizzato non differisce molto. La differenza riguarda, invece, le tempistiche ai fini di rendere edotta l'autorità giudiziaria e la convalida successiva da parte di essa delle misure provvisorie e del sequestro della stampa. Difatti, all'articolo 13 si prevede una tempistica di quarantottore, mentre per quanto riguarda la stampa, invece, la tempistica è dimezzata. Il dettato dell'articolo 21 sembra far intendere, dunque, come la libertà di manifestazione del pensiero sia su un gradino più alto rispetto alla libertà personale a livello di tutela immediata. Al di là di questo aspetto, il principio fondamentale statuito dall'art.21 è il diritto per chiunque di manifestare liberamente il proprio pensiero attraverso qualsiasi mezzo di diffusione assicurando una tutela a tutto tondo a tale diritto. I costituenti, poi, erano consapevoli che in futuro ci sarebbe stato uno sviluppo dei mezzi di comunicazione, pertanto, è ragionevole la clausola aperta posta a conclusione del primo comma, la quale statuisce "*[…] e ogni altro mezzo di diffusione"*[265]. L'unico limite esplicito presente ai fini di una restrizione della libertà di pensiero è rappresentato dal buon costume come previsto al comma quarto. È un limite non troppo stringente, in quanto il concetto stesso di buon costume è mutevole con il tempo, pertanto non è un qualcosa di definitivo. La libertà tutelata dall'articolo 21, inoltre, è fondamentale in quanto rappresenta l'elemento portante della democrazia, ossia il pluralismo ideologico. Attraverso uno scambio continuo di idee, opinioni e visioni diverse è possibile dare vita ad un dialogo costruttivo che consente, ai rappresentanti in Parlamento, di prendere

[264] Gometz, 2017
[265] Art.21 co.1 Costituzione

la decisione *migliore* che accontenti la maggioranza e che dia la possibilità alla minoranza di esprimersi in senso contrario. Pluralismo ideologico che si traduce, poi, in una democrazia che ha i connotati della tolleranza e dell'apertura al diverso. A titolo di esempio, è rilevante l'ordinanza del Tribunale di Roma del 12 dicembre 2019 con la quale il Giudicante ha accolto il ricorso di CasaPound Italia ordinando la riattivazione della pagina Facebook del partito oltre ad una serie di sanzioni[266]. Ciò che rileva dalla ordinanza in questione è il ruolo che assume la piattaforma social, in quanto viene riconosciuto come l'esclusione del soggetto ricorrente da essa comporti all'emarginazione dal dibattito politico testimoniato, anche, dal fatto che la maggior parte degli esponenti politici utilizza quotidianamente Facebook per la diffusione dei messaggi politici e delle idee del proprio movimento[267]. Tale esclusione, dunque, andrebbe a violare il pluralismo dei partiti politici come previsto dall'articolo 49 della Costituzione, nonché la libertà di espressione impedendo ai rappresentanti di CasaPound di diffondere le loro idee politiche. Emerge, dunque, come la libertà di opinione possa essere limitata ma come ogni sua limitazione deve essere controbilanciata dalla tutela di un valore ritenuto superiore per quella determinata circostanza. Questa vicenda dimostra come la Costituzione si fondi su una democrazia aperta e tollerante, pronta ad accogliere anche il dissenso includendo nel dibattito politico coloro che in un senso o nell'altro andrebbero contro i valori democratici promossi dalla Carta fondamentale. Si è detto come i padri costituenti abbiano considerato, nella tutela della libertà in oggetto, qualsiasi mezzo di diffusione del pensiero. In questa nozione vi rientrano, dunque, anche Internet e i social network. È ormai pacifico come tali mezzi siano uno strumento potentissimo di comunicazione consentendo un dialogo immediato, diretto e senza intermediari. A tal proposito, ormai da più di un decennio si discute della possibilità di inserire il diritto di accesso ad Internet attraverso l'aggiunta di un nuovo articolo nel testo costituzionale o di un nuovo comma all'articolo 21 che preveda tale diritto. Nel 2010 vi era stato un primo disegno di legge costituzionale, il n.2485, nel quale vi era la proposta di aggiungere l'articolo 21 bis al testo costituzionale con la seguente formulazione ad opera di Stefano Rodotà, uno dei maggiori esponenti in materia: "*Tutti hanno eguale diritto di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire le violazioni dei diritti di cui al Titolo I della parte I"*[268]. Attraverso questo dettato normativo, dunque, vengono ribaditi il principio di uguaglianza formale e sostanziale riprendendo l'articolo 3 della Costituzione e il principio di personalità sancito all'articolo 2. È chiaro come Internet costituisca uno strumento che consente di godere in un contesto più ampio i propri diritti e libertà fondamentali, in

[266] Tribunale di Roma - https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/01/sentenzacpifb.pdf
[267] *Ibidem*
[268] Senato, si veda https://www.senato.it/service/PDF/PDFServer/BGT/00519114.pdf

primis la libertà di espressione. La Rete, difatti, è vista come un mezzo di proiezione e sviluppo della persona come individuo, ma anche all'interno di un contesto sociale in riferimento alle *communites, fandom* et similia che si creano in Rete, come verrà poi successivamente ripreso nella Dichiarazione dei diritti in Internet del 2015, di cui uno degli autori è proprio l'illustre professore Rodotà. In questa prima proposta di modifica al testo costituzionale, si è posta attenzione non solo al diritto di accedere in condizioni paritarie ad Internet, ma anche all'aspetto delle infrastrutture e dei mezzi necessari per poter garantire tale diritto. A tal proposito, nel testo della proposta di legge vi è il suggerimento, ai fini dell'accesso ad Internet, di sviluppare e implementare una banda larga per superare il divario tra le zone rurali e le zone urbane. Considerando il periodo, ossia il 2010, ciò non deve stupire in quanto si era nella piena fase di evoluzione nell'ambito digitale con la nascita di nuove tecnologie e di nuovi strumenti di comunicazione sempre più sofisticati. Il tema della costituzionalizzazione del diritto di accesso ad Intenet nello scorso decennio era un tema caldo, in quanto a pochi anni di distanza vi fu la redazione di un ulteriore proposta di legge costituzionale, ossia la numero 2816 del 2015[269]. A differenza della precedente, tale proposta inserisce il diritto di accesso ad Internet subito dopo l'articolo 34 della Costituzione tutelante il diritto all'istruzione nel titolo II, il quale disciplina i rapporti etico – sociali. L'articolo 34-bis veniva formulato in tali termini: "*Tutti hanno uguale diritto di accedere alla rete Internet, in modo neutrale, in condizioni di parità e con modalità tecnologicamente adeguate. La Repubblica promuove le condizioni che rendono effettivo l'accesso ad Internet come luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale"*[270]. La formulazione è meno sintetica rispetto alla proposta del 2010 risultando, quindi, più dettagliata nel contenuto. L'attenzione, in tale formulazione, è posta sull'accesso ad Internet come diritto sociale attraverso una costituzionalizzazione dell'obbligo da parte dello Stato di fornire tutti i mezzi e le infrastrutture necessarie affinché il singolo possa sviluppare la propria personalità e partecipare alle formazioni sociali riprendendo, dunque, il principio personalistico sancito all'articolo 2. I cittadini, dunque, secondo quanto affermato nella proposta di legge, vanterebbero nei confronti dello Stato un diritto potestativo, ossia una pretesa affinché l'apparato statuale provveda in tal senso. La libertà di espressione e la tutela della democrazia, poi, sarebbe rafforzata dal diritto di accesso ad Internet, in quanto si verrebbe a concretizzare la democrazia elettronica fornendo ai cittadini "*gli strumenti per informarsi, seguire e controllare l'operato dei loro rappresentanti ed essere quindi in grado di porre […] istanze e domande alla politica"*[271]. Si realizzerebbe, per così dire, una sorta di Big Brother al contrario. Infine, solo due anni fa vi fu l'ultima proposta di legge costituzionale in

[269] Camera, si veda http://documenti.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0028730.pdf
[270] *Ibidem*
[271] *Ibidem*

materia, n.327[272], nascente dalle esigenze che si sono acuite con la pandemia, in primis la didattica a distanza e lo *smart working*, ma anche dal fatto che il diritto di accesso ad Internet viene visto come uno *"spartiacque tra inclusione ed esclusione sociale"*[273]. In questo caso non viene aggiunto un nuovo articolo al testo costituzionale, ma un nuovo comma all'articolo 21 statuente: "*Tutti hanno eguale diritto di accedere alla rete Internet, in condizioni di parità, con modalità tecnologicamente adeguate tali da favorire la rimozione di ogni ostacolo di ordine economico e social. La legge stabilisce provvedimenti adeguati a prevenire le violazioni del diritto di cui al presente comma".* Il presente testo è molto simile alla formulazione della proposta di legge costituzionale del 2015 configurando tale diritto come un diritto sociale, ossia come una pretesa del cittadino ad ottenere da parte dello Stato infrastrutture e un sistema di telecomunicazioni che sia adeguato, affinché tutti possano esercitare online i propri diritti e sfruttare i servizi offerti dalla Pubblica Amministrazione, andando così, a costituire ciò che viene identificato nell'*e-government.* Nonostante vi siano state numerose proposte di legge costituzionali volte a costituzionalizzare il diritto di accesso ad Internet identificato di volta in volta come pretesa del cittadino nei confronti dello Stato ad ottenere un sistema di telecomunicazioni ed infrastrutture adeguate per superare il divario tra zone rurali e zone urbane, nonché come strumento per sviluppare la propria personalità anche in un contesto digitale andando, di conseguenza, a rafforzare la libertà di espressione e il pluralismo democratico, le suddette proposte non sono mai andate a buon fine. Non è stata ravvisata, probabilmente, la necessità di introdurre l'accesso a Internet come diritto costituzionale, nonostante a livello internazionale ciò è ampiamente riconosciuto[274], in quanto l'articolo 21 della Costituzione garantisce la libertà di manifestare il proprio pensiero con qualsiasi mezzo come espresso in chiusura al primo comma. Inoltre, gli articoli 2 e 3 della Costituzione sarebbero già sufficienti a garantire lo sviluppo dell'individuo nelle formazioni sociali e condizioni di parità che possono essere applicate anche al mondo digitale. Per tali ragioni, dunque, tali progetti di riforma costituzionale non sono andati in porto. Diritto al voto, diritto di esprimere le proprie opinioni senza correre il rischio della censura sono solo alcune forme di tutela della democrazia nel contesto dei diritti fondamentali. Il collante che consente di poter esercitare liberamente tali diritti è rappresentato dalla libertà di associazione come disciplinata all'articolo 18 della Costituzione. Associarsi, generalmente, vuol dire costituire un'organizzazione stabile tra persone che condividono uno scopo comune. Un esempio di associazione sono i partiti politici, tutelati dall'articolo 49 il quale riconosce il diritto di associazione politica. Il dettato normativo, poi, pone alcuni limiti a tale libertà. In primis i fini perseguiti dall'associazione non devono essere vietati dalla legge, altrimenti si rischia

[272] Camera, si veda http://documenti.camera.it/leg19/pdl/pdf/leg.19.pdl.camera.327.19PDL0008910.pdf
[273] *Ibidem*
[274] Si veda a tal proposito l'ONU e l'OCSE.

di ricadere nelle fattispecie di reato di associazione a delinquere, disciplinato dall'articolo 416 c.p. o dell'associazione a delinquere di stampo mafioso ex articolo 416 bis c.p. Il secondo comma pone ulteriori due limiti, ossia l'associazione non deve essere segreta[275] e non deve perseguire scopi politici attraverso un'organizzazione di tipo militare. Tale limite è alquanto rilevante, poiché fa comprendere come in un regime democratico i fini politici devono essere perseguiti con mezzi pacifici e non attraverso mezzi violenti, i quali potrebbero, invece, sovvertire l'ordine democratico. È facile comprendere il perché questa libertà sia il collante che consente l'esercizio del diritto al voto e il manifestare liberamente il proprio pensiero. Per quanto riguarda il primo punto, se i cittadini non avessero la possibilità di riunirsi pacificamente allora non potrebbero nemmeno dare vita ai partiti politici, elemento portante della forma di governo democratica che garantisce il pluralismo. La libertà garantita dall'articolo 18, poi, è strettamente correlata con l'articolo 21, in quanto il trovarsi in un luogo fisico o virtuale per scambiarsi idee, opinioni, ma anche esprimere il proprio dissenso rappresenta una delle tante forme di associazione. Si comprende, dunque, come ad oggi la democrazia abbia connotati diversi a seconda della *funzione* che è chiamata a perseguire. Ma non solo. Democrazia oggi vuol dire anche partecipazione politica sotto diverse forme, da quella più tradizionale a quella che cerca di guardare al futuro e al mondo digitale. Democrazia, poi, significa anche tutela dei diritti fondamentali, i quali pur essendo un concetto relativamente recente, trovano spazio non solo a livello internazionale, ma anche interno grazie alla nostra Costituzione. In conclusione, quindi, ad oggi parlare di democrazia significa ragionare su concetto estremamente complesso, ricco di sfumature e in continua evoluzione.

[275] Si intende per associazioni segrete quelle che "*anche all'interno di associazioni palesi, occultando la loro esistenza ovvero tenendo segrete congiuntamente finalità e attività sociali ovvero rendendo sconosciuti, in tutto od in parte ed anche reciprocamente, i soci, svolgono attività diretta ad interferire sull'esercizio delle funzioni di organi costituzionali, di amministrazioni pubbliche, anche ad ordinamento autonomo, di enti pubblici anche economici, nonché di servizi pubblici essenziali di interesse nazionale*" secondo quanto previsto dall'articolo 1 della legge n.17 del 25 gennaio 1982.

CAPITOLO III: IL CONCETTO DI E-DEMOCRACY.

1. La nozione di e-democracy

Si è visto come il concetto di democrazia non sia statico, ma mutevole a seconda del periodo storico di riferimento e dei cambiamenti di carattere economico, sociale e culturale che si verificano con il passare del tempo. Oltre a questi fattori bisogna considerare anche i progressi tecnologici e come essi abbiano condotto ad una riflessione sulla possibilità di utilizzare le tecnologie della comunicazione e dell'informazione nell'ambito dei processi democratici. L'unione tra le ICT e i processi decisionali ha dato vita al concetto di democrazia elettronica detta altrimenti *e-democracy.* Si può pensare che sia un concetto relativamente recente, in realtà già a partire dalla fine della seconda guerra mondiale si iniziò a riflettere su questo tema, grazie alla nascita e allo sviluppo delle scienze cibernetiche con Norbert Wiener[276]. Negli anni '50 del secolo scorso, in piena Guerra fredda, la corsa agli armamenti e la necessità di continui progressi in qualsiasi campo, soprattutto quello tecnologico, portò a considerare l'utilizzazione dei computer nel settore politico. In questa prima fase di teorizzazione della democrazia elettronica si è compreso come la società fosse sempre più complessa e come potesse usufruire di un sistema computerizzato di informazioni[277]. I computer, dunque, vengono concepiti come potenziali intermediari tra la società e la politica in quanto erano e sono in grado di processare numerose quantità di dati e giungere a conclusioni più razionali[278]. Si osserva come in questa fase è del tutto assente un approccio di tipo personale inteso nel senso di un dialogo tra cittadino e politico. L'approccio iniziale alla democrazia elettronica, dunque, è di tipo razionale e scientifico[279]. Nelle due decadi successive viene effettuato un passo in avanti a seguito dei movimenti sociali che si stavano diffondendo per tutto il globo giungendo ad una visione diversa della politica. Vi è una società attiva che scende in campo per rivendicare i propri diritti, soprattutto le donne[280]. In questo periodo si registrano dei progressi, in quanto per la prima volta entrano nelle case la TV via cavo e i *personal computers*. Non è ancora nato Internet, si dovrà aspettare il decennio successivo, ma la presenza di questi due strumenti ha fatto sì

[276] Norbert Weiner è stato un matematico e statistico statunitense. È il fondatore della cibernetica, ossia una scienza che si occupa del controllo dei macchinari tramite computer e dello studio del cervello e del sistema nervoso e del rapporto tra i due sistemi. Egli definì la cibernetica come "*proprietà della macchina di agire e di reagire agli stimoli ambientali".* Si veda Moro, 2022.
[277] Floridia, 2015
[278] Vedel, 2006
[279] *Ibidem*
[280] Negli anni '70 del secolo scorso si assiste alla seconda ondata del movimento femminista incentrato sul tema della liberazione femminile. In Italia, in questo periodo con la legge n.898 del 1970 e con la legge n.194 del 1978 vengono garantiti rispettivamente il diritto al divorzio e il diritto all'aborto.

che venissero messe in onda le prime trasmissioni di dibattito politico, i primi talk show e ciò ha comportato un enorme cambiamento nella politica. Si realizza, così, la cc.dd. *teledemocracy,* ossia l'utilizzazione da parte degli attori politici della televisione come mezzo di comunicazione[281]. Si giunge, infine, allo sviluppo compiuto del concetto di democrazia elettronica nella ultima decade del secolo scorso con la Internet Revolution e la presenza di nuovi mezzi di comunicazione nei primi anni 2000 con la nascita dei social network. Vi è un'ondata di ottimismo circa l'utilizzazione di Internet, in quanto chiunque è in grado di esprimere la propria opinione e diffondere le proprie idee nella dimensione del *cyberspazio,* ossia un luogo non fisico in cui vi è uno scambio di interazioni e il consolidamento di relazioni nel web. Come scritto nella *Dichiarazione d'indipendenza del cyberspazio* da John Perry Barrow "*Ours is a world that is both everywhere and nowhere, but it is not where bodies live"*[282] ossia il mondo del *cyberspazio* è immateriale presente ovunque dove non vivono i corpi. Parlare di democrazia elettronica non è fantascientifico, infatti nel 1984 Carl Schmitt e Norberto Bobbio avevano prospettato l'utilizzazione di strumenti tecnologici che consentissero al cittadino di esprimere la propria opinione su una questione politica[283]. Per il filosofo italiano si può parlare di *computer – crazia,* ossia "*la possibilità di trasmettere il proprio voto ad un cervello elettronico"*[284]. Entrambi gli autori prevedono l'utilizzazione di strumenti tecnologici che consentono l'espressione del proprio voto o della propria opinione su una determinata questione. Ma non solo. Schmitt e Bobbio mettono in guardia circa le conseguenze di questa nuova forma di democrazia, ossia il verificarsi di un *eccesso di democrazia*[285]*,* in quanto verrebbe a concretizzarsi la democrazia diretta. Schmitt, infatti, nel suo scritto osserva come attraverso questo meccanismo non si avrebbe un'opinione coesa, ma *una somma di opinioni private*[286] che non necessariamente rappresentano l'opinione pubblica. Sarebbe, dunque, un'illusione il poter raggiungere la *miglior* decisione per la comunità, ossia frutto di un bilanciamento tra posizioni diverse attraverso tali strumenti, in quanto ognuno potrebbe ritenere che il proprio credo sia quello giusto da seguire e dunque andrebbe a confrontarsi solo con altri individui che condividono lo stesso parere. Si sono, dunque, anticipati in una sorta di profezia le conseguenze dell'utilizzazione della tecnologia nei processi democratici precedendo ciò che Cass Sunstein ed Eli Pariser individuano nei fenomeni delle *echo chambers* e delle *filter bubbles*[287]. Schmitt e Bobbio,

[281] Rivera, 2017
[282] Barlow, 1996
[283] Schmitt, 1984
[284] Bobbio, 1984
[285] *Ibidem*
[286] Schmitt, 1984
[287] Per echo chambers si intendono delle camere virtuali in cui vengono vi sono gruppi di persone che interagiscono tra di loro condividendo opinioni simili rispetto ad un determinato tema. Le filter bubbles, invece, sono il risultato della personalizzazione dei contenuti presenti nelle piattaforme social facendo sì che gli utenti vengano maggiormente esposti ai contenuti che confermano le loro opinioni o che siano correlate ad esse.

dunque, ritengono che il realizzarsi di questa nuova forma di democrazia non sia un progresso, ma un passo indietro. Nonostante la presenza di qualche voce, seppur autorevole, a sfavore della democrazia elettronica si è comunque cercato di definire questo fenomeno, in quanto non si può negare che la tecnologia sia una componente essenziale nella vita dell'uomo contemporaneo. La necessità di inquadrare tale fenomeno nasce dall'esigenza di dare un significato per quanto possibile univoco all'espressione *e-democracy,* poiché spesso viene confusa con altri concetti, ossia l'*e-governance,* l'*e-government* e il voto elettronico[288].

In letteratura sono presenti una varietà di definizioni di democrazia elettronica, ai fini di questo studio si considera la nozione fornita da Gianmarco Gometz, secondo il quale la democrazia elettronica consiste "[nel]*l'uso delle ICT come mezzo per lo svolgimento delle procedure egualitarie di autogoverno del demos"*[289]. In primis viene immediatamente in risalto lo strumento attraverso il quale si realizza l'*e-democracy,* ossia le tecnologie dell'informazione e della comunicazione. A causa degli aggettivi che vengono associati a democrazia, tale termine può assumere innumerevoli significati e ciò porta al smarrimento dell'elemento essenziale, vale a dire l'autogoverno del popolo. L'Autore, invece, pone attenzione su tale aspetto incorporandolo nella definizione stessa di democrazia elettronica per non correre il rischio di chiamare democrazia qualcosa che in realtà non lo è. Uno dei principi fondamentali, recepiti anche nella nostra Costituzione, è l'eguaglianza tra cittadini. Gometz nel definire il fenomeno della democrazia elettronica considera anche questo aspetto riferendosi alle *procedure egualitarie.* Questo aspetto è strettamente correlato con l'autogoverno del popolo, ossia ognuno deve essere messo nella condizione di partecipare alla vita politica dello Stato partendo da una condizione di parità senza fare alcun tipo di distinzione. Si comprende, allora, che all'interno del mare magnum di definizioni date circa il concetto di democrazia elettronica la strada migliore da perseguire sia quella di una definizione minimale, in quanto si adatta in base alle circostanze per cui tale concetto non riguarda solamente la partecipazione elettorale vera e propria, ma si estende anche a tutte le fasi antecedenti e preparatorie alle elezioni*,* quali, ad esempio, comizi e campagne elettorali. Scegliere una nozione minima di democrazia elettronica fa sì che tale concetto assuma valenza universale. Anche a livello sovranazionale il tema della democrazia elettronica è presente. A tal proposito vi è la risoluzione del Parlamento europeo del 16 marzo 2017 *"E-democrazia nell'Unione Europea: potenziale e sfide".* In breve, la risoluzione affronta il tema della democrazia elettronica constando il fatto che tale nozione è frutto di cambiamenti sociali, economici e culturali riscontrando una partecipazione ridotta e un costante aumento dell'astensionismo. Osservando i dati e prendendo in considerazione solamente

[288] Il voto elettronico è uno strumento alternativo alla scheda compilativa che permette al cittadino di esprimere la propria preferenza attraverso tecnologie informatiche e telematiche.
[289] Gometz, 2017

l'Italia si è registrato un notevole calo di affluenza alle urne per l'elezione del Parlamento europeo. Nel 1979, anno dal quale si tengono le elezioni per la rinnovazione degli organi dell'UE, l'85,65% degli aventi diritto al voto si è presentato. Nella decade successiva, l'81,07%. Infine, alle ultime elezioni tenutesi nel 2019 solo il 54,50% ha votato[290]. Nell'arco di quarant'anni, dunque, vi è stato un calo di oltre il 30%. Tale astensionismo è causato da una pluralità di fattori, quali apatia nei confronti della politica, ma anche una mancata consapevolezza sul ruolo del Parlamento europeo. Malgrado i dati statistici e i cambiamenti di carattere economico e sociale, il Parlamento europeo vede nella democrazia elettronica il mezzo più adatto per aumentare la partecipazione dell'elettorato ai processi decisionali non solo a livello sovranazionale, ma anche nazionale. Le ICT, infatti, sarebbero in grado di contribuire alla cittadinanza attiva migliorando la trasparenza e la responsabilità nel processo decisionale[291]. L'istituzione europea è anche conscia delle sfide che la democrazia elettronica pone, soprattutto in riferimento a uno dei mezzi con cui essa si realizzerebbe, ossia il voto elettronico. Vi è il rischio di distorsioni e manipolazioni dei risultati, ma ciò può essere evitato se vi è la fiducia dei cittadini nelle istituzioni e nei processi democratici, da un lato, e un'educazione digitale dei cittadini, dall'altro, che permetta loro di poter essere in grado di utilizzare nel modo corretto gli strumenti preposti al voto elettronico e migliorare le proprie competenze in materia di ICT[292]. Alla luce di tali riflessioni, dunque, si coglie l'essenza della democrazia elettronica. L'*e-democracy* non è un fenomeno facilmente inquadrabile, nonostante si cerchi di dare una definizione il più minimale possibile. Si può affermare come *e-democracy* possa essere considerata un'espressione piuttosto ampia che racchiude in sé diverse tematiche, soprattutto di carattere filosofico – sociologico consistenti nella riflessione circa l'impatto delle ICT sui processi democratici. Colonna portante della democrazia elettronica, infatti, è l'utilizzazione delle ICT e dei nuovi mezzi di comunicazione per ridurre l'astensionismo e favorire una cittadinanza attiva. La domanda di fondo che sorge spontanea è la seguente: attualmente, grazie al costante progresso tecnologico e allo sviluppo di nuovi mezzi di comunicazione è concretamente realizzabile la democrazia elettronica? Detto in altri termini, la democrazia rappresentativa è arrivata al capolinea? A tale quesito non è possibile dare una risposta certa, poiché vi sono argomenti a sostegno, ma anche argomenti a sfavore, i quali condividono considerazioni sull'utilizzo della tecnologia nei processi democratici.

[290] https://www.europarl.europa.eu/election-results-2019/it/affluenza/
[291] Risoluzione del Parlamento europeo del 16 marzo 2017 sulla e-democrazia nell'Unione europea: potenziale e sfide (2016/2008(INI))
[292] *Ibidem*

1.1. Vantaggi e svantaggi dell'*e-democracy*

Il concetto di *e-democracy* presenta alcuni aspetti positivi, ma anche dei lati oscuri che in questo breve paragrafo si cercherà di individuare. Per quanto riguarda gli argomenti a favore dell'*e-democracy* il tutto è riassumibile nel cyber ottimismo, il quale realizzerebbe la visione della dimensione politico – utopistica della datificazione. Vi è questa correlazione, in quanto grazie all'utilizzo delle tecnologie civiche si realizzerebbe l'*empowerment,* vale a dire il potenziamento della collettività, inteso come autonomizzazione dal potere che utilizza la tecnologia per manipolare le masse a proprio piacere. La diffusione delle ICT contrasterebbe tale potere, in quanto si affermerebbe un contropotere che è libero, diffuso e massificato e per tali caratteristiche necessariamente buono[293]. Il cyber ottimismo, poi, si spinge oltre ritenendo che grazie al continuo progresso tecnologico in un futuro non molto lontano verrà a realizzarsi la democrazia diretta. Difatti, grazie all'utilizzo delle ICT si avrebbe un continuo dialogo con l'elettorato, il quale manifesterebbe le proprie preoccupazioni ed esigenze al corpo politico facendo sì che, a seguito di un continuo monitoraggio, non sia più necessario un corpo intermedio in quanto i cittadini sarebbero messi nella condizione di prendere una decisione, il che si traduce in autogoverno in senso stretto, ossia democrazia diretta. Grazie alla democrazia elettronica, inoltre, si realizzerebbe la dottrina della saggezza della moltitudine, ossia il popolo metterebbe in comune le proprie conoscenze ed esperienze affinché si sia in grado prendere la *miglior* decisione per la collettività. Sull'onda di questo ottimismo nei confronti della *e-democracy* si considerano, poi, i vantaggi che la Rete può fornire. In primis, verrebbe ridotta l'asimmetria informativa in quanto il singolo è in grado di informarsi e ha il diritto di essere informato sui temi trattati dalla politica. Grazie all'informazione il singolo è messo nella condizione di poter vagliare le tesi sostenute, le opzioni a disposizione affinché venga effettuata una scelta consapevole. La Rete, poi, ha in sé una vocazione liberale[294], difatti si parla di *net freedom.* Internet, secondo questa prospettiva, è uno strumento di valorizzazione e di accrescimento delle libertà dell'individuo. A tal proposito, nel 2015 la Commissione per i diritti e i doveri relativi a Internet ha elaborato la *Dichiarazione dei diritti in Internet* un documento di quattordici articoli che mira a disciplinare i diritti dell'individuo in Internet. In particolare, l'articolo 2 rubricato *Diritto di accesso* al primo comma prevede l'accesso a Internet come "*diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale"*[295]. Si prende coscienza del fatto che la Rete ha notevolmente ampliato i diritti presenti in

[293] Sarra, 2022
[294] Frosini, 2017
[295] Commissione per i diritti e i doveri relativi ad Internet, 2015

Costituzione, come la libertà di espressione che trova spazio nei social network, blog e forum oppure il diritto al lavoro che trova spazio nei siti web, ad esempio Indeed e nei social, come Linkedin, per la ricerca e l'offerta di lavoro. L'individuo in Rete viene tutelato come nell'art.2 della Costituzione, ossia come singolo e nelle formazioni sociali. La Rete, dunque, è un'estensione della personalità dell'individuo il quale deve essere messo nelle condizioni di potervi accedere per potersi sviluppare come individuo e nelle formazioni sociali online. Per garantire ciò, il secondo comma dell'art.2 prevede l'uguaglianza sostanziale all'accesso[296]. Altro esempio di accrescimento della libertà dell'individuo in rete è fornito dall'articolo 3 della Dichiarazione rubricato *Diritto alla conoscenza e all'educazione in rete.* Nel dettaglio, il comma 3 statuisce "*Ogni persona ha il diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali*[297]*".* L'educazione digitale è lo strumento principale che consente di usufruire al massimo le potenzialità e i contenuti della Rete. Educazione che si rende necessaria per navigare nel mare magnum di informazioni presenti in Internet per poter sviluppare un pensiero critico ed essere in grado di valutare l'attendibilità di quanto letto sui social e sulle principali piattaforme di informazione digitale. Malgrado questa vocazione liberale vi è da considerare come possano essere eretti dei muri digitali attraverso il meccanismo della censura. Tale fenomeno si riscontra soprattutto nelle democrazie illiberali nelle quali viene negato l'accesso a Internet al *demos* o viene in qualche misura limitato[298]. Si mettono in atto pratiche come la cancellazione di parole, di nomi e di espressioni chiave nei motori di ricerca che impediscono alla cittadinanza di essere in contatto con il mondo reale e di documentarsi. Ciò, dunque, conferma la natura liberale della Rete, in quanto tali pratiche dimostrano come per le democrazie illiberali Internet sia una minaccia, poiché verrebbe messo in discussione il concetto di sovranità[299]. Internet, infatti, è una fonte di accesso al mondo esterno che dà la possibilità ai cittadini di documentarsi facendo, dunque, vacillare la strumentalizzazione dei social e della Rete da parte del Governo. Sono presenti, poi, argomenti contro la democrazia elettronica che possono essere riassunti nel declino del cyber ottimismo, in quanto l'utilizzazione delle ICT e della tecnologia nei processi democratici anche se rivoluzionaria non comporta, in realtà, ad un cambiamento del paradigma in quanto sono dei mezzi che si affiancano alla democrazia rappresentativa. Non si può, poi, negare l'impatto delle ICT in senso negativo. La politica ha compreso come siano uno strumento potentissimo

[296] Articolo 2 della Dichiarazione dei diritti in Internet: *"Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale".*
[297] Commissione per i diritti e i doveri relativi ad Internet, 2015
[298] Frosini, 2017
[299] *Ibidem*

di comunicazione con l'elettorato, dunque, vi potrebbe essere un uso distorto tramite la diffusione di fake news e teorie che urlano al complotto. Inoltre, la democrazia elettronica realizzerebbe quanto paventato da Bobbio e Schmitt, ossia l'*eccesso di democrazia* con conseguente indebolimento delle istituzioni rappresentative che risulterebbero essere prive di utilità. La presenza di intermediari, invece, è necessaria, poiché sono in grado di favorire un dialogo aperto al confronto con posizioni e visioni diverse per poter, poi, prendere le decisioni più adatte al fine di perseguire gli interessi della maggioranza. A tale assunto, però, si può sollevare un'obiezione, ossia non ci sarebbe un indebolimento delle istituzioni rappresentative, in quanto Internet è solo un mezzo di diffusione di informazioni, di teorie e di idee. Il momento decisionale rimane il voto[300]. Si può, tuttavia, facilmente ribattere che, anche se il voto è il momento decisionale, il cittadino arriva alle elezioni *biased,* ossia la sua preferenza è influenzata da una serie di fattori di natura endogena ed esogena. I primi sono attinenti alla persona e si possono individuare, ad esempio, nel credo politico, nell'iniziativa ad informarsi e nell'essere in grado di valutare l'attendibilità delle informazioni lette nel web. I fattori esogeni, invece, riguardano l'ambiente in cui è immerso l'individuo. Si possono considerare come fattori esogeni, ad esempio, l'esposizione ad una pluralità di informazioni, il confronto vis à vis di posizioni diverse, la propria rete di informazioni, *talk show* di attualità etc. L'unione di questi elementi fa sì che l'elettore arrivi alle urne con una propria idea e consapevolezza formatesi grazie a diversi canali informazionali, tra cui la Rete. Internet è luogo non solo di informazione, ma di disinformazione e ciò ha portato in tempi recenti alla diffusione dei movimenti populisti che credono nel potere diretto del popolo e nell'assenza di rappresentanti in Parlamento realizzando, di fatto, la democrazia diretta andando ad indebolire le istituzioni rappresentative. La Rete, dunque, è il tramite attraverso cui si realizza l'*eccesso di democrazia.* Un ulteriore argomentazione a sfavore della democrazia elettronica è di carattere costituzionale, ossia l'*e-democracy* ostacolerebbe i processi deliberativi mediati dall'interazione tra elettorato e rappresentanti e non si potrebbe comunque realizzare in quanto vi sarebbe un contrasto insanabile con l'art.67 della Costituzione[301], ossia il divieto di mandato imperativo. Il nostro ordinamento prevede tale divieto, in quanto il parlamentare "*rappresenta la Nazione"*[302], ossia egli rappresenta il popolo nella sua interezza, oltre agli interessi particolari di chi lo ha eletto. Vi è un contrasto tra democrazia elettronica e divieto di mandato imperativo, in quanto l'*e-democracy* metterebbe in pratica la democrazia diretta, la quale trova un ostacolo proprio nell'art.67 della Costituzione. Se si prospetta, in futuro, l'attuazione della democrazia elettronica sarebbe necessario, dunque, compiere un processo di disintermediazione, il che implica un processo di revisione

[300] *Ibidem*
[301] Gallo, 2020
[302] Art.67 Costituzione

costituzionale che, al momento, non sembra prospettabile e che nell'ipotesi in cui dovesse essere proposto difficilmente avrà successo, poiché significherebbe modificare l'intero assetto istituzionale della democrazia parlamentare che l'Italia conosce da più di settant'anni. È un cambiamento eccessivo, per cui la soluzione migliore sarebbe un'implementazione graduata nel rispetto delle forme e dei limiti della Costituzione determinando come e quando gli aventi diritto al voto possano usare le ICT per fini decisionali[303].

La democrazia rappresentativa, dunque, è arrivata al capolinea? A seguito delle argomentazioni riportate sia a favore sia contro l'*e-democracy* ciò che emerge è un quadro della situazione piuttosto complesso che rende difficile prendere una posizione a riguardo. Gli argomenti a favore corrono il rischio di peccare di un eccessivo ottimismo nei confronti dell'utilizzazione della tecnologia nei processi democratici. Le voci contrarie all'*e-democracy,* invece, malgrado sollevino delle problematiche di particolare rilevanza incorrono nel rischio di demonizzare le ICT e la tecnologia non vedendoli come potenziali alleati che contribuirebbero ad avvicinare la cittadinanza alla politica, e ad essere più attiva, ma come una minaccia alla democrazia.

Si possono, dunque, individuare due posizioni. Vi è chi non vede di buon occhio la democrazia elettronica e paventa un cambiamento sancito dall'abbandono del modello tradizionale della democrazia rappresentativa ritenendo, invece, che tale sia la miglior forma di governo poiché viene garantita una mediazione tra forze politiche opposte che non si raggiungerebbe con l'*e-democracy.* Vi è, d'altronde, chi è più ottimista e vede l'utilizzo delle ICT e della tecnologia come potenziali alleati e non come una minaccia e non esclude che in futuro la democrazia elettronica si realizzi a determinate condizioni e nel rispetto dell'assetto istituzionale delineato dalla Costituzione.

1.2. E-government, e-governance

Le ICT non trovano applicazione solamente nell'ambito della partecipazione politica e dei processi decisionali, ma anche nel settore della Pubblica Amministrazione con l'obiettivo di fornire servizi digitali e promuovere una cittadinanza attiva. L'utilizzazione delle ICT in tale settore si riferisce *all'e-government* e all'*e-governance*, termini spesso confusi con il concetto di democrazia elettronica. Vi è questa sovrapposizione di termini, in quanto sono concetti che sono nati e sviluppati in contemporanea ai cambiamenti socioeconomici e all'avvento delle nuove tecnologie e dei nuovi mezzi di comunicazione. Queste innovazioni non riguardano solo l'aspetto teorico in riferimento alla concettualizzazione dell'*e-democracy*, ma anche l'aspetto pratico, vale a dire l'utilizzazione in concreto delle nuove tecnologie nel settore della Pubblica Amministrazione per assicurarne una

[303] Gometz, 2017

maggiore efficienza, trasparenza e imparzialità. Dato il rischio di una potenziale sovrapposizione fra *e-democracy*, *e-government* ed *e-governance*, in letteratura sono presenti una varietà di definizioni che consentono di tracciare i confini tra questi concetti. Nel dettaglio, l'*e-government* è un fenomeno di cui si è occupata fin dai primi anni 2000 la Commissione europea, ex Commissione delle comunità europee, la quale nel 2003 ha rilasciato una comunicazione intitolata "*Il ruolo dell'eGovernment per il futuro dell'Europa"*. Con questo documento, la Commissione europea riflette sull'*e-government* e di come sia necessario per la Pubblica Amministrazione adeguarsi ai cambiamenti socioeconomici in atto e all'impatto delle tecnologie in tale settore. L'*e-government* nella prospettiva europea viene identificato come "*l'uso delle ICT nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche"*[304]. Da questa definizione emerge l'utilizzo delle ICT affinché vi sia un mutamento nell'organizzazione della Pubblica Amministrazione consentendone un miglioramento in termini di prestazioni. In particolare, nella comunicazione emerge come la digitalizzazione della Pubblica Amministrazione gioverebbe i cittadini andandone a migliorare la qualità della vita, in quanto verrebbe garantita una maggiore trasparenza e "*apertura delle pubbliche istituzioni"*[305]. La Commissione europea, poi, rileva come tale processo sia fondamentale affinché anche la democrazia stessa ne esca rafforzata, poiché grazie a strumenti come i forum online e il voto elettronico i cittadini sono in grado di esprimere il loro punto di vista e far valere le loro istanze ai rappresentanti politici contribuendo, dunque, al processo democratico. Un ulteriore definizione di *e-governement* è fornita dalle Nazioni Unite, le quali individuano l'*e-governement* nell'utilizzazione delle ICT per fornire in maniera più efficiente i servizi della Pubblica Amministrazione ai cittadini e alle imprese. L'obiettivo dell'*e-government* è quello di fornire servizi migliori, rispondere alle esigenze dei cittadini circa la trasparenza e la *accountability* ed essere maggiormente inclusivi[306]. A differenza della Commissione europea, la definizione fornita dalle Nazioni Unite è più ampia, in quanto individua tre modelli di *e-government*, ossia (i) il Government to Government, (ii) il Government to Business ed infine (iii) il Government to Consumer o to Citizen[307]. Dei vantaggi dell'*e-government* ne tratta, poi, la *World Bank,* la quale afferma come i benefici di un governo elettronico si racchiudono in maggiore trasparenza, riduzione della corruzione, crescita del fatturato per le imprese

[304] Commissione delle comunità europee, 2003
[305] *Ibidem*
[306] United Nations, definizione di *e-government.*
[307] Per quanto riguarda il primo modello, esso coinvolge la condivisione dei dati e scambi elettronici tra gli attori del Governo. Inoltre, il Government to Government prevede uno scambio tra agenzie governative a livello nazionale e a livello provinciale e locale. Il Government to Business, invece, prevede l'utilizzo delle ICT per la realizzazione di transazioni come pagamenti e acquisti di beni e servizi e la fornitura di servizi online, come gli e-commerce. Il terzo modello, infine, prevede iniziative progettate per favorire l'interazione tra cittadini e Pubblica Amministrazione. Si veda United Nations, definizione di *e-government.*

e una riduzione dei costi[308]. Se si volessero individuare, dunque, gli elementi principali dell'*e-government* tali possono essere identificati nell'utilizzazione delle ICT e delle più recenti tecnologie nel settore della Pubblica Amministrazione per renderla più efficiente e trasparente nei confronti dei cittadini che sono in grado, grazie al processo di digitalizzazione della PA, di usufruire di servizi online da essa fornita. Le definizioni date finora presentano come elemento comune la trasparenza della Pubblica Amministrazione. Tale principio è presente a livello sovranazionale all'articolo 15 co.1 del Trattato sul funzionamento dell'Unione Europea il quale statuisce *"Al fine di promuovere il buon governo e garantire la partecipazione della società civile, le istituzioni, gli organi e gli organismi dell'Unione operano nel modo più trasparente possibile".* L'operare *nel modo più trasparente possibile* implica che chiunque, cittadino dell'Unione e non, ha la possibilità di accedere ai documenti delle istituzioni e delle agenzie dell'Unione, ma non solo[309]. Per quanto riguarda, invece, il principio di trasparenza a livello interno, l'art.22 della legge sul procedimento amministrativo[310] prevede il diritto di accesso ai documenti della Pubblica Amministrazione, ossia il "*diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi"*[311]. Tale diritto si pone come prerogativa per migliorare la trasparenza dell'attività della Pubblica Amministrazione, in quanto i cittadini hanno la possibilità di visionarne i documenti e di ottenere informazioni anche per quanto riguarda eventuali procedimenti a loro carico[312]. Si evince, dunque, un profondo legame tra il concetto di *e-government* e il principio di trasparenza, il quale si evolve nell'*open government.* Per *open government*[313] come definito dall'OECD nel 2016*,* che tradotto significa *governo aperto,* si intende una cultura di governance "*che promuove i principi di trasparenza, integrità, accountability e*

[308] World Bank, si veda https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government

[309] Per quanto attiene alla trasparenza a livello sovranazionale, essa è garantita tout court per cui vi è la possibilità di consultare la banche dati dell'Unione, come EUR-lex per la consultazione dei testi legislativi e registri pubblici delle varie istituzioni come quelli del Parlamento europeo o della Commissione.

[310] Legge del 7 agosto 1990 n.241

[311] Art.22 legge del 7 agosto n.241/1990

[312] In riferimento ad eventuali contenziosi amministrativi, il diritto di accesso ai documenti è fondamentale, in quanto il ricorrente coinvolto in un processo amministrativo può trovarsi nella situazione di non avere a disposizione un documento che, invece, è detenuto dalla Pubblica Amministrazione che potrebbe essere utile ai fini dell'attività istruttoria. Per tal ragione, dunque, è previsto tale diritto: non solo per aumentare la trasparenza e l'imparzialità dell'operato della Pubblica Amministrazione, ma anche per consentire alla parte debole del processo, ossia il ricorrente, ad ottenere documenti il cui contenuto potrebbe essere fondamentale ai fini della risoluzione della controversia garantendo, così, anche il diritto di difesa.

[313] Un esempio di open government è il memorandum del 2009 di Barak Obama, il quale intende promuovere la trasparenza essenziale per rafforzare la democrazia e l'efficienza del Governo. In particolare, la trasparenza, secondo il memorandum, promuove l'*accountability,* ossia il rendere conto del Governo e della Pubblica Amministrazione ai cittadini del loro operato. A seguito di tale memorandum, nello stesso anno fu creato il portale web data.gov il quale consente a chiunque di accedere ai dati pubblicati da agenzie di tutto il governo federale raggruppati in diverse categorie e con diversi criteri, quali, ad esempio, argomento e popolarità. Si veda https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government, 2009

partecipazione dei portatori d'interesse[314] *a supporto della democrazia e della crescita inclusiva"*[315]. In particolare, l'*open government* in virtù del principio di trasparenza si traduce nel rendere disponibili gratuitamente informazioni e dati pubblici che siano completi, aggiornati e attendibili. Inoltre, il cittadino deve essere in grado di reperire tali dati facilmente minimizzando *lo* sforzo di consultazione[316]. Nel nostro ordinamento in ossequio alla trasparenza della PA e dell'*open government* si potrebbe fare riferimento non solo alle legge sul procedimento amministrativo, ma anche al diritto di accesso civico come disciplinato all'art.5 del D.lgs. n.33/2013. Al primo comma viene disciplinato l'accesso civico semplice, ossia l'obbligo che permane in capo alle Pubbliche amministrazioni di pubblicare "*documenti, informazioni o dati"*[317] su richiesta di chiunque nel caso in cui sia stata ommessa la loro pubblicazione. È, dunque, un rimedio all'inosservanza dell'obbligo di pubblicazione da parte della P.A. Il secondo comma, invece, prevede l'accesso civico generalizzato, il quale consiste nel diritto di chiunque di accedere a dati e documenti detenuti dalla P.A., ulteriori rispetto a quelli previsti dal decreto in questione[318]. Vi sono, però, dei limiti indicati nell'art.5-bis che ne impediscono l'accesso per tutelare interessi di carattere pubblico e per evitare di recare pregiudizio ad interessi di natura privata[319].

L'*e-governance*, invece, condivide con l'*e-government* l'utilizzo delle ICT nel settore della Pubblica Amministrazione, ma secondo il Consiglio d'Europa l'obiettivo è quello di migliorare tramite queste tecnologie la qualità dei servizi offerti dal Governo a cittadini e imprese[320]. Per l'UNESCO, invece, l'*e-governance* consiste nell'esercizio dell'autorità politica, economica e amministrativa nella gestione degli affari di Stato tramite l'utilizzo delle ICT per facilitare il processo di diffusione delle

---

[314] Per portatori di interesse si intende in generale la cittadinanza.

[315] OECD, si veda https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/Racc_Consiglio_sul_Governo_Aperto.pdf

[316] *Ibidem*

[317] Art.5 co.1 D.lgs. n.33/2013 statuisce *"L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione".*

[318] Art.5 co.2 D.lgs. n.33/2013 afferma *"Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis".*

[319] A tutela dell'interesse pubblico, il diritto di accesso, come previsto dall'art.5-bis del D.lgs. n.33/2013, viene negato per tutelare: (i) la sicurezza pubblica e l'ordine pubblico, (ii) la sicurezza nazionale, (iii) la difesa e le questioni militari, (iv) le relazioni internazionali, (v) la politica e la stabilità finanziaria ed economica dello Stato, (vi) la conduzione di indagini sui reati e il loro perseguimento, (vii) il regolare svolgimento delle attività ispettive. A tutela degli interessi privati, invece, il diritto di accesso viene negato per (i) la protezione dei dati personali, in conformità con la disciplina legislativa in materia, (ii) la libertà e la segretezza della corrispondenza, (iii) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

[320] Consiglio d'Europa

informazioni al pubblico[321]. Il risultato, dunque, è una maggiore trasparenza e responsabilità del Governo e della Pubblica Amministrazione nei confronti della cittadinanza. Visti così, *e-government* ed *e-governance* sembrano concetti simili, se non uguali in quanto condividono l'utilizzo delle ICT nel settore pubblico e il principio di trasparenza. In realtà, l'*e-governance* è un concetto più ampio che racchiude l'*e-government*, poiché considera l'impatto che hanno le tecnologie dell'informazione e della comunicazione nella fornitura da parte delle Pubbliche Amministrazione di servizi online e, in generale, sul rapporto tra governanti e governati[322]. L'*e-government*, invece, è strettamente correlato alla fornitura di servizi governativi online e non comprende, dunque, una prospettiva più ampia che riguarda anche lo studio delle conseguenze delle ICT nel settore pubblico, in quanto come obiettivo principale si pone il miglioramento dell'efficienza e trasparenza della Pubblica Amministrazione. Alla luce delle definizioni considerate è possibile, dunque, delineare un confine tra *e-democracy*, *e-government* ed *e-governance*. Per democrazia elettronica si intende l'utilizzo delle ICT nei processi di partecipazione politica e decisionali al fine di superare la cc.dd. crisi della democrazia rappresentativa. L'*e-government*, invece, riguarda l'impiego delle ICT nel settore pubblico per la fornitura alla cittadinanza di servizi online al fine di migliorare l'efficienza, la trasparenza e l'imparzialità della Pubblica Amministrazione. L'*e-governance* si distingue dall'*e-government*, poiché è un concetto molto più ampio che non riguarda solo la prestazione di servizi online, ma anche riflessioni sull'impatto che le nuove tecnologie hanno avuto nel rapporto tra pubblico e Governo. Per quanto riguarda questo ultimo aspetto, è possibile effettuare una riflessione sull'utilizzo delle ICT nel settore pubblico e vagliare i possibili vantaggi, nonché le criticità presenti. Non vi è dubbio che le ICT abbiano comportato nel settore pubblico una serie di benefici in termini di organizzazione della struttura stessa della Pubblica Amministrazione migliorandone l'efficienza e riducendo notevolmente la burocrazia. Il cittadino che necessita di un determinato servizio non deve più recarsi presso l'ente di riferimento,

[321] UNESCO, si veda https://webarchive.unesco.org/20161021003528/http:/portal.unesco.org/ci/en/ev.php-URL_ID=4404&URL_DO=DO_TOPIC&URL_SECTION=201.html

[322] L'e-government è un concetto più ampio che è influenzato anche dallo lo sviluppo delle nuove tecnologie e dal mutamento dei costumi sociali. In particolare si possono individuare quattro fasi. Il punto di partenza è determinato dall'Internet Revolution negli anni '90 del secolo scorso, poiché è solo con la nascita di Internet e la sua massificazione che si inizia a riflettere sulla possibilità di impiegare le ICT in vari settori, tra cui quello pubblico. Fino al 2005 si registra una fase di passaggio di trasformazione dall'analogico al digitale con la diffusione dei *personal computers*, stampanti, e-mail ed SMS. Dal 2005 al 2009 vi è il periodo del boom dei social network con la nascita di Facebook e Twitter e con la valutazione dei primi modelli di e-governance. Fino al 2012, poi, l'attenzione si concentra sui social. Ci si rende conto di come la comunicazione con la cittadinanza sia mutata notevolmente e di come i diversi canali social siano in grado di raggiungere un'enorme fetta di pubblico. Non vi è da negare, poi, come in questo periodo stesse emergendo anche la consapevolezza di un potenziale uso distorto dei nuovi mezzi di comunicazione e la possibilità di una loro strumentalizzazione da parte degli operatori politici. Venendo, poi, al presente nell'ultimo decennio vi è stato uno sviluppo circa lo studio dell'utilizzazione delle ICT nei processi democratici e la concettualizzazione di *e-government* e di *e-governance*. Si è registrata, inoltre, una massificazione della tecnologia e una riduzione nel costo dei device elettronici che ha contribuito ad intensificare la continua evoluzione della comunicazione tra corpo politico e cittadinanza. Per ulteriori dettagli si consulti Fornasier, 2021.

ma può accedere al portale web e presentare la propria istanza e avviare il procedimento. La Pubblica Amministrazione, poi, deve essere il più trasparente possibile, in quanto le informazioni devono essere facilmente ricercate online da chiunque vi abbia interesse e ciò è un fattore di responsabilizzazione verso il pubblico. Un ulteriore vantaggio consiste nell'utilizzare le nuove tecnologie a disposizione per far fronte ad una serie di problematiche che riguardano gli aspetti della privacy e della protezione dei dati del cittadino. Difatti, il semplice accesso ai portali web delle Pubbliche Amministrazioni o l'accesso a SPID[323], a titolo di esempio, comporta l'inserimento di dati sensibili quali e-mail, codice fiscale o numero di cellulare. È evidente, poi, che per la fornitura dei servizi online i portali web delle varie agenzie e amministrazioni a livello centrale e locale raccolgono enormi quantità di informazioni che vengono utilizzate successivamente per facilitare le iniziative di *e-government*[324]. Sorge, dunque, la necessità di utilizzare adeguate misure per l'archiviazione dei dati per evitare, come è successo in tempi recenti[325], attacchi informatici che rischiano di diffondere dati sensibili di migliaia di utenti, nonché informazioni riservate coperte dalla disciplina del segreto. Una soluzione a tale problematica è fornita dall'impiego della blockchain nel settore dell'*e-government* e dell'*e-governance*. Grazie alle sue caratteristiche, tra cui la trasparenza, l'immutabilità e la resilienza si evita potenzialmente tale scenario. Tali caratteristiche risultano essere preziose per il settore pubblico, poiché garantiscono un elevato livello di sicurezza del sistema. Per quanto riguarda la trasparenza, ogni operazione che viene effettuata nella rete è immediatamente visibile a tutti i partecipanti del network per cui ogni tentativo di manipolazione dei blocchi è evidente. A ciò, dunque, si collega l'immutabilità. Difatti, una volta inseriti i dati all'interno della catena e una volta convalidata la transazione non è più possibile effettuare alcuna modifica. Se si volesse operare in tal senso, sarebbe necessario effettuare una nuova transazione e aggiungere un nuovo blocco alla catena. Infine, la resilienza è l'aspetto più rilevante ai fini dell'*e-government* e dell'*e-governance*, poiché è una proprietà della blockchain che garantisce il funzionamento del sistema, anche in un ipotetico attacco informatico. Su questo punto, qualora vi fosse un attacco informatico e uno o più nodi non dovessero funzionare ciò non inficerebbe sul funzionamento complessivo della blockchain, poiché sono presenti tutti gli altri nodi detentori di una copia delle transazioni effettuate fungendo, dunque, da backup. Questa caratteristica è rilevante proprio perché consente ai portali di fornitura di servizi online di funzionare anche in condizioni avverse. Malgrado gli aspetti positivi dell'utilizzazione delle nuove tecnologie, tra cui la blockchain, per l'implementazione dell'*e-government* e dell'*e-governance* bisogna considerare anche alcune criticità.

[323] È il sistema pubblico di identità digitale che permette l'accesso ai servizi digitali delle amministrazioni locali e centrali.
[324] Phadke, Medrano e Ustymenko, 2022
[325] Da quanto emerge dal report della Polizia postale, nel 2023 vi è stato un calo del 7% di attacchi cyber rispetto al 2022 a istituzioni e imprese con matrice il conflitto russo-ucraino e la guerra nel cyberspazio per assicurarsi il dominio. Si veda https://www.ilsole24ore.com/art/nel-2023-11930-attacchi-cyber-7percento-diramati-oltre-75mila-alert-AFzxSuCC

In primis, non vi è alcuna certezza sul fatto che i sistemi informatici non siano bersaglio di attacchi informatici che ne ostano il corretto funzionamento con il conseguente rischio di *data leak,* ossia di diffusione di dati sensibili anche se vi è l'utilizzazione delle più recenti tecnologie e dei più avanzati sistemi di sicurezza. Altro aspetto da non sottovalutare, poi, è l'inadeguatezza delle infrastrutture presenti. Difatti, si verificano spesso problemi tecnici che impediscono al cittadino di accedere ai servizi online forniti dalla Pubblica Amministrazione. Dal punto di vista sociale, infine, vi è il rischio di creare una nuova classe di esclusi, ossia soggetti privi di un'educazione digitale che non sono in grado di utilizzare strumenti della quotidianità come computers e smartphone, o che sono privi di tali mezzi e quindi non sono in grado di usufruire dei servizi digitali offerti. Si tratta, dunque, del problema del digital divide. Agli inizi dell'Internet Revolution e della nascita dei social tale ostacolo era più evidente, in quanto vi era uno scarto fra generazioni, ossia quella dei nostri nonni e dei nostri genitori. Oggi, invece, il dilemma del digital divide è meno presente, poiché le differenze tra generazioni si stanno assottigliando sempre di più. Dalle brevi riflessioni sul punto, dunque, si evince come le nozioni di *e-democracy, e-government* e *e-governance* non debbano, anzi, non possano essere confuse in quanto afferiscono a concetti diversi tra loro.

2. Perché si parla di e-democracy

Vista la nozione di *e-democracy,* la quale consiste nell'impiego della tecnologia e delle ICT nei processi di partecipazione politica e decisionali con l'obiettivo di risanare il legame intercorrente tra l'elettorato e la classe politica a fronte di una perdurante crisi della democrazia rappresentativa, sorge la necessità di indagare le ragioni che hanno portato alla teorizzazione di tale concetto nell'attuale contesto politico – giuridico considerando i cambiamenti sociali, politici e culturali che si sono verificati negli ultimi decenni. Il punto di partenza della trattazione approfondirà le cause principali che hanno portato alla crisi della democrazia rappresentativa per, poi, proseguire sulla constatazione del sempre maggior utilizzo dei social network all'interno del contesto politico e di come ciò abbia comportato ad un profondo cambiamento nel rapportarsi con l'elettorato analizzando gli effetti delle cc.dd. *filter bubbles* ossia delle bolle di filtro e delle cc.dd. *echo chambers*, ovvero delle camere di eco, nonché l'emergere del populismo. Malgrado vi siano delle perplessità circa l'implementazione in un futuro prossimo della democrazia elettronica, si può affermare come siano presenti anche delle voci a sostegno che ne auspicano una futura concretizzazione nel rispetto dei limiti previsti dall'assetto costituzionale e dall'ordinamento.

2.1. Crisi della democrazia rappresentativa e dei partiti politici

In greco il verbo *krino* significa tagliare, separare ma anche giudicare e discernere. Da *krino* deriva il termine crisi, il quale viene associato ad un evento negativo poiché rappresenta la rottura dell'equilibrio dello stato delle cose che porta ad una condizione di turbamento temporaneo. Crisi, dunque, rappresenta una rottura rispetto allo status quo ante. Nell'ambito politico si parla ormai da decenni di crisi della democrazia rappresentativa e dei partiti politici. È interessante osservare come il linguaggio della politica prenda in prestito alcuni termini dal linguaggio medico, in quanto in letteratura non si fa solo riferimento alla crisi, ma anche ad uno status di malessere generale della democrazia rappresentativa, un qualcosa di patologico che necessita di cure e rimedi adeguati. I fattori che hanno generato questo status di malessere generale possono essere individuati principalmente nei mutamenti del tessuto sociale e nello sviluppo delle ICT e della tecnologia. Lo sviluppo in termini tecnologici ha fatto sì che vi fosse un profondo cambiamento nella comunicazione tra corpo politico e corpo elettorale grazie all'utilizzo della televisione e dei social network, oltre ad aver contribuito alla trasformazione dei partiti politici dando vita ai cc.dd. partiti outsider o partiti antisistema.

Lo stato di malessere generale della democrazia rappresentativa si riscontra su più fronti. In primis, dal punto di vista storico, in Italia il sistema ha mostrato i primi segni di cedimento a partire dal 1992 con Tangentopoli, ossia una serie di inchieste che hanno preso il via con l'arresto di Mario Chiesa il 17 febbraio 1992 colto in flagrante mentre stava intascando una tangente di sette milioni di lire. È stato uno shock culturale per l'intero Paese, il quale è venuto a conoscenza dell'enorme giro di tangenti che finanziavano illecitamente i partiti in cambio di appalti e accordi per le imprese che le versavano. Bettino Craxi nel suo celebre discorso al Parlamento affermò "*Buona parte del finanziamento politico è irregolare o illegale. Non credo che ci sia nessuno in quest'aula, responsabile politico di organizzazioni importanti, che possa alzarsi e pronunciare un giuramento in senso contrario a quanto affermo*"[326] a riprova del fatto che tutti erano a conoscenza del fenomeno corruttivo in atto. È la retorica del chi non ha commesso alcun peccato scagli per primo una pietra. Con Tangentopoli, infatti, crolla la cc.dd. Prima Repubblica e crollano le certezze che si erano affermate. Con la cc.dd. Seconda Repubblica, inaugurata dalle elezioni politiche del 1994 con la vittoria di Silvio Berlusconi, si registra un profondo cambiamento, poiché da un lato si è cercato di dare un nuovo aspetto al partito, il quale risulta sempre più personalizzato e concentrato non tanto sul programma elettorale ma sulla figura del *leader*, dall'altro grazie alla rivoluzione tecnologica in atto vi è stata una trasformazione nel modo di approcciarsi all'elettorato sfruttando nuovi strumenti di comunicazione, tra cui la televisione. Se nell'età premoderna vi era una comunicazione tramite stampa di partito, manifesti elettorali e

[326] Si veda https://tg24.sky.it/cronaca/approfondimenti/tangentopoli-protagonisti-mani-pulite#04

mobilitazione degli iscritti tipico dei primi del '900, con il passare del tempo la comunicazione si è evoluta e all'epoca della Seconda Repubblica si è nel pieno di una rivoluzione televisiva. La comunicazione è più diretta, vi sono spot che promuovono i partiti e i loro programmi elettorali, ma soprattutto la comunicazione comincia ad essere capillare e a raggiungere fette di pubblico che nella precedente fase non era possibile raggiungere[327]. Nonostante vi sia una comunicazione massificata, gli elettori da soggetti attivi interessati alla vita politica del Paese si sono trasformati in soggetti passivi. Essendo una rivoluzione televisiva si può affermare come l'elettore si sia trasformato in uno spettatore che non è più intenzionato a sviluppare un'intelligenza politica, per cui appare disinteressato e più incline a non presentarsi alle urne. L'astensionismo, infatti, è uno dei sintomi di una democrazia le cui condizioni di salute peggiorano ad ogni elezione. A titolo di esempio, se alle consultazioni elettorali del 1976 il tasso di partecipazione elettorale era pari al 93,39%, alle ultime elezioni del 25 settembre 2022 si è registrata una presenza alle urne pari al 67,8%[328]. Nell'arco di quattro decadi vi è stato un calo di circa venticinque punti percentuali in riferimento all'affluenza alle urne, un dato piuttosto allarmante. L'astensionismo, però, è un fenomeno che presenta diverse sfumature. A tal proposito si può fare una distinzione tra astensionismo apparente e astensionismo reale. Per astensionismo apparente si fa riferimento alle differenze presenti tra le varie fonti normative[329] che disciplinano l'elettorato attivo, soprattutto in riferimento alle diverse tipologie di consultazioni elettorali[330]. L'astensionismo reale, invece, riguarda le motivazioni che portano l'elettorato a non presentarsi alle urne[331]. In particolare, per quest'ultimo aspetto si fa riferimento ad una serie di fattori che impediscono al cittadino – elettore di recarsi alle urne, come problemi motori che lo impossibilitano a muoversi o il semplice fatto di non risiedere momentaneamente o in maniera permanente nel territorio della propria circoscrizione. Ragioni, dunque, che non dipendono da una apatia del soggetto nei confronti della politica, ma che sono rappresentative delle difficoltà fisiche in senso proprio e in senso figurato dell'elettore che non gli consentono di esercitare il diritto al voto. Per fronteggiare tale problematica, dunque, nel libro bianco sull'astensionismo si sono elaborate alcune proposte. Una di queste è il cc.dd. *election pass,* ossia la digitalizzazione della tessera e delle liste elettorali[332]. L'*election pass*, dunque, andrebbe a sostituire la tessera elettorale ed evitare il rischio di un possibile smarrimento, in quanto

[327] Raniolo & Tarditi, 2021
[328] https://www.openpolis.it/lastensionismo-e-il-partito-del-non-voto/
[329] Si veda, ad esempio, la legge costituzionale n.1 del 17 febbraio 2000 che ha riconosciuto il diritto al voto per i cittadini italiani residenti all'Estero, oltre alla legge del 27 dicembre 2001 n.459 che disciplina il voto per corrispondenza. Inoltre, per i cittadini italiani residenti all'Estero che vogliano partecipare alle elezioni europee è previsto all'art.3 del d.l. n.408 del 24 giugno 1994 convertito nella legge n.483 del 3 agosto 1994 la possibilità di votare nelle sezioni costituite presso i consolati, gli istituti di cultura, le scuole italiane e altri locali messi a disposizione dagli Stati membri.
[330] Bassanini, 2022
[331] *Ibidem*
[332] *Ibidem*

verrebbe direttamente scaricato sullo smartphone e avviato da una apposita applicazione. L'*election pass* potrebbe essere un valido strumento per contrastare tale fenomeno, ma vi è da ritenere che possano insorgere dei problemi a livello di sicurezza informatica. Potrebbe, poi, essere presente la criticità del digital divide, problema di natura secondaria in quanto non sarebbe una misura obbligatoria per tutti, oltre al fatto che le differenze tra una generazione e l'altra si stanno assottigliando sempre di più. Nel libro bianco si prosegue, poi, all'analisi di alcune varianti del voto come antidoto per l'astensionismo come il voto per corrispondenza riservato ai cittadini residenti all'estero[333] o il voto anticipato presidiato[334].

Ulteriore elemento che ha contribuito a mettere in crisi le odierne democrazie rappresentative è lo sviluppo delle ICT e la diffusione di Internet che ha concorso a mutare la relazione tra classe politica ed elettorato, nonché la struttura stessa dei partiti con l'emersione dei cc.dd. partiti digitali. Si è in una nuova era della comunicazione politica, ossia quella *data driven*[335] guidata dai dati raccolti da varie piattaforme digitali tramite l'osservazione del comportamento online dell'utente. Nel mondo del web ogni giorno vengono prodotte infinite quantità di dati utilizzati per le più svariate finalità, tra cui anche la profilazione. Per profilazione si intende una qualsiasi forma di trattamento automatizzato dei dati personali, i quali vengono impiegati per la valutazione o la predizione di alcuni aspetti di una persona come, ad esempio, la situazione economica, le preferenze personali, gli interessi o i suoi spostamenti[336]. La profilazione, dunque, è frutto di una raccolta di dati personali dell'utente i quali vengono elaborati tramite mezzi tecnologici che sono in grado di prendere una decisione in assenza di un coinvolgimento umano per trarre, analizzare o prevedere alcuni aspetti personali del soggetto sottoposto a tale trattamento. Tutto ciò è possibile grazie alla presenza dei *big data,* ossia l'insieme dei dati raccolti da diverse fonti tali da essere così vasti e complessi da dover essere processati dalle più

[333] È la modalità di voto garantita per i cittadini italiani residenti all'estero disciplinata dalla legge n.459/2001. All'articolo 12 viene descritta la modalità con cui il cittadino esprime il proprio voto. Non oltre diciotto giorni dalla data stabilita per le votazioni in Italia, gli uffici consolari inviano agli elettori ammessi al voto per corrispondenza il plico contenente il certificato elettorale, la scheda elettorale e due buste. La prima nella quale verrà inserita la scheda elettorale e la seconda che è affrancata recante l'indirizzo dell'ufficio consolare competente. Il plico contiene poi le istruzioni su come esprimere la propria preferenza di voto e la lista dei candidati. L'elettore, una volta espresso il voto, introduce nella apposita busta la scheda elettorale e la sigilla per poi inserirla nella busta affrancata. La busta poi dovrà essere inviata non oltre il decimo giorno precedente alla data stabilita per le votazioni in Italia. La legge prescrive, poi, che le buste non devono recare alcun segno di riconoscimento a tutela della segretezza e libertà del voto.

[334] Modalità di voto che consente all'elettore di votare in giorni diversi da quelli previsti per la votazione in seggi allestiti nella località di residenza o in località diverse.

[335] Raniolo & Tarditi, 2021

[336] Articolo 4 n.4 Regolamento n.679/2016. Il testo integrale riporta: "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

recenti tecnologie, come l'intelligenza artificiale[337]. Il loro utilizzo può essere destinato a più finalità, ossia per scopi descrittivi, predittivi o prescrittivi[338]. Nell'era *data driven,* dunque, grazie ad una massiccia utilizzazione dei dati prodotti dagli utenti su diverse piattaforme digitali risulta possibile una personalizzazione dell'attività di campagna elettorale. È noto il caso Cambridge Analytica[339], società statunitense che ha sfruttato i dati personali degli utenti Facebook per indirizzarli verso la campagna elettorale che fosse il più compatibile possibile con i loro interessi e il loro credo politico. L'utilizzo dei *big data* non deve essere demonizzato, in quanto essi possono essere un'enorme risorsa soprattutto per poter predire eventi futuri, scoprire nuove tendenze e prendere le *giuste* decisioni al *momento giusto*, il che è fondamentale in politica. Il problema, piuttosto, risiede nel modo con cui tali dati vengono raccolti e processati, ossia in maniera non del tutto trasparente e all'insaputa del diretto interessato. L'attività politica per poter sfruttare a proprio favore i *big data* necessita di nuove figure professionali quali *data analyst,* ossia professionisti del settore che analizzano e raggruppano i dati ma anche *social media manager,* i quali si occupano di costruire la strategia di comunicazione più adatta per un'organizzazione, un'impresa o una persona fisica. Il loro ruolo è fondamentale, in quanto sono coloro che si occupano della gestione del profilo social, della creazione dei contenuti e il monitoraggio delle interazioni e condivisioni. L'analisi di commenti, interazioni, condivisioni e *likes* permette di valutare l'approvazione del pubblico nei confronti di specifici punti del programma elettorale e consente di prevedere il grado di accoglienza che potrebbero ricevere ulteriori proposte. L'emersione di nuovi mezzi di comunicazione e di nuove tecnologie ha comportato, dunque, ad una professionalizzazione dell'attività politica, la quale vede coinvolti sempre di più professionisti del settore *social* e un cambiamento nel modo di relazionarsi con il corpo elettorale. Su questo punto si osserva come i social siano un ottimo strumento, in quanto la comunicazione risulta essere capillare e grazie all'utilizzo di algoritmi, *big data* e adeguate strategie di marketing è possibile raggiungere

[337] Tratto da https://www.europarl.europa.eu/topics/it/article/20210211STO97614/big-data-definizione-benefici-e-sfide-infografica

[338] La finalità descrittiva ha come obiettivo la raccolta dei dati per descrivere una determinata situazione e *visualizzare i principali indicatori di prestazione*. La finalità predittiva risulta essere la più utile nell'ambito della politica, poiché si tratta di utilizzare i dati raccolti per prevedere con un certo anticipo l'accadimento di eventi futuri. Infine, la finalità prescrittiva è anch'essa utile in politica in quanto permette di valutare e quantificare l'effetto delle future decisioni prima di effettuare una determinata scelta. Si veda Coniglione, 2023.

[339] Cambridge Analytica è una società fondata nel 2013 da Robert Mercer specializzata nella raccolta ed elaborazione dei dati ottenuti dai profili degli utenti nelle principali piattaforme online. L'obiettivo è creare un profilo ad hoc osservando il comportamento online dell'utente per poi sottoporlo alla pubblicità altamente personalizzata. La società è stata coinvolta nello scandalo delle elezioni presidenziali del 2016, in quanto avrebbe raccolto dati di milioni di utenti Facebook senza consenso, in quanto i dati sono stati raccolti attraverso l'applicazione creata da Aleksandr Kogan, ossia *thisisyourdigitallife,* la quale creava il profilo psicologico dell'utente e la previsione del proprio comportamento basandosi sulle attività svolte online. Ai fini del suo utilizzo, gli utenti vi accedevano tramite Facebook Login. Attraverso questa applicazione sono stati raccolti i dati di chi vi aveva fatto l'accesso, ma anche dei loro amici per poi essere trasmessi a Cambridge Analytica. I dati così ottenuti poi sono stati utilizzati per creare pubblicità mirata che fosse coincidente con il profilo creato e sono stati creati, durante la campagna elettorale di Trump del 2016, numerosi account *fake* e *bot* allo scopo di diffondere notizie false e altri contenuti volti a mettere in cattiva luce l'avversaria, ossia Hilary Clinton. Si veda Menietti, 2018.

grandi fette di pubblico[340]. L'utilizzo di questi canali di comunicazione alternativi a quelli tradizionali non ha un impatto del tutto negativo, poiché le piattaforme *social* consentono una comunicazione veloce, economica e immediata tramite un linguaggio più accessibile a tutti, altrimenti l'elettore non sarebbe in grado di ricevere il messaggio trasmesso dal corpo politico[341]. Le nuove tecnologie, poi, hanno contribuito a modificare la struttura stessa dei partiti dando vita ai cc.dd. partiti outsider, i quali sfruttano al meglio le piattaforme digitali per potersi affermare nel contesto dei partiti tradizionalmente intesi. Sono partiti che si identificano come partiti antisistema, i quali sono portatori di valori diversi da quelli promossi dall'ordinamento politico di cui fanno parte, tant'è che ne prendono le distanze[342]. Vi è la condivisione di uno schema comune che consente di individuare gli elementi caratteristici di questi nuovi partiti che approdano in politica. I partiti outsider sono, per lo più, partiti di matrice populista i quali, dunque, si oppongono all'establishment individuandolo come nemico da contrastare. Tale tipologia di partiti, poi, non disprezzano la democrazia, in quanto sfruttano la tecnologia a disposizione per attivare istituti di democrazia diretta. Questa nuova tipologia di partito è riuscito sapientemente a sfruttare la Rete e le nuove tecnologie per potersi affermare come alternativa ai partiti tradizionalmente intesi. Attraverso blog e forum, infatti, i leader di questi partiti entrano in diretto contatto con gli iscritti cogliendone le istanze, critiche e spunti per poter arricchire il programma politico. Vi è, quindi, una condivisione di idee, la quale può essere identificata nel cc.dd. *marketplace of ideas,* ossia nel credo che le idee debbano circolare liberamente e competere tra loro, affinché possano emergere le migliori[343]. La Rete, dunque, consente una partecipazione più attiva del cittadino e andrebbe a contrastare quell'apatia nei confronti della politica che risulta essere uno dei sintomi del malessere generale della democrazia rappresentativa. Malgrado siano presenti innumerevoli vantaggi della Rete vi è da considerare il rischio di una *socialcrazia,* ossia una affermazione dei social network nei processi decisionali che, se non è adeguatamente controllata ha come conseguenza il superamento della barriera della rappresentanza andando a depotenziare il ruolo del Parlamento nella definizione

[340] Un chiaro esempio di come i social siano una componente essenziale, per certi versi, nella politica di oggi è rappresentato dalle recenti elezioni del 2022 e la diffusione tra i politici della piattaforma *Tiktok*. Questo social viene utilizzato soprattutto dai più giovani, dunque, dotarsi di un profilo per promuovere il proprio programma elettorale risulta una mossa vincente per raggiungere l'elettorato più giovane. A titolo di esempio, l'attuale Presidente del Consiglio aveva postato un video in cui teneva in mano dei meloni affermando: "*25 settembre, ho detto tutto".* Si consulti https://www.rainews.it/video/2022/09/il-video-di-giorgia-con-due-meloni-alla-vigilia-del-voto-d56bb707-b6db-4bca-a503-a2fee5ae270e.html

[341] Un chiaro esempio di come l'utilizzazione dei social nell'ambito politico non sia solo un *male,* ma una fonte preziosa sono le dirette Facebook dell'allora Presidente del Consiglio Giuseppe Conte tenute quasi ogni sera per annunciare il lockdown e le novità in merito nonché quali zone fossero rosse, arancioni o gialle specificando le attività che potevano essere eseguite e le attività, invece, vietate. È stato un punto di svolta, poiché per la prima volta si è abbandonata la comunicazione televisiva a reti unificate con la mediazione dei giornalisti. Si consulti Amoretti & Santaniello, 2021.

[342] Ferrari, 2015

[343] Parafrasando quanto affermato da Giovanni De Gregorio nel saggio *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?* Si veda https://www.medialaws.eu/wp-content/uploads/2019/05/9.-De-Gregorio.pdf

della politica nazionale[344]. Si realizzerebbe, dunque, la tanto paventata democrazia diretta e l'eccesso di democrazia come teorizzato da Bobbio e da Schmidt.

Riassumendo, dunque, il quadro clinico che la democrazia rappresentativa presenta esso è connotato da una serie di sintomi a cui si è cercato di provvedere con alcuni rimedi. In primis, la democrazia rappresentativa risulta entrare in crisi a seguito dei cambiamenti economici e sociali avvenuti negli anni '90 del secolo scorso a partire dalla vicenda Tangentopoli. Si può affermare come tale sia stato il momento cruciale in cui l'elettorato ha iniziato a perdere la fiducia nel corpo politico che lo rappresenta in Parlamento. L'astensionismo, dunque, risulta essere la naturale conseguenza della sfiducia nella classe dirigente, la quale ha cercato di rimediare a tale distacco e di entrare in sintonia con l'elettorato, soprattutto quello più giovane, sfruttando i canali social come *TikTok.* Tecnologia che ha avuto un impatto fondamentale nell'aggravare il quadro clinico, in quanto attraverso la raccolta di dati personali e la loro elaborazione si è violata all'insaputa dell'utente la sua privacy, affinché potesse essere sottoposto ad una pubblicità mirata durante la campagna elettorale. L'uso delle ICT e delle nuove tecnologie, poi, ha contribuito alla trasformazione dei partiti tradizionalmente intesi facendo emergere il fenomeno dei partiti antipartito e il rischio di una democrazia dei social in cui ognuno può esprimere la propria idea e diventare *leader* di opinione facendo venire meno, al contempo, il filtro della rappresentanza e il medium tra corpo elettorale e corpo politico. Un quadro, dunque, che non è molto rassicurante. Non è facile, però, individuare la miglior medicina che possa far guarire la democrazia rappresentativa dai suoi malanni. Si è visto che *l'e-democracy* può essere una valida alternativa alla democrazia rappresentativa, ma al momento non è la soluzione migliore poiché vi sono ostacoli all'interno dell'ordinamento, la Costituzione in primis, che ne impedirebbero attualmente l'implementazione. Il nostro legislatore ha tentato di prestare soccorso con la recente riforma costituzionale sulla riduzione del numero dei parlamentari modificando gli articoli 56 e 57 della Costituzione riducendo il numero dei parlamentari da 945 a 600 con un taglio di 345 parlamentari e una riduzione della spesa di circa 500 milioni di euro a Legislatura[345]. È necessario riflettere, seppur in breve, su questa riforma alquanto discussa e discutibile. Intervenire sulla rappresentanza politica andando a ridurre il numero dei parlamentari non è, probabilmente, la soluzione migliore per fronteggiare la crisi della democrazia rappresentativa. La ragione principale per cui tale riforma è piuttosto discutibile risiede nel fatto che vi è un deficit di rappresentanza non indifferente, soprattutto per le piccole Regioni alle quali spetta un numero limitato di parlamentari, di conseguenza vi è il rischio che vengano eletti solo i deputati e i senatori della maggioranza[346]. Deficit di rappresentanza

[344] Rivera, 2017
[345] Si vada su https://www.riformeistituzionali.gov.it/it/la-riduzione-del-numero-dei-parlamentari/
[346] Piraino, 2020

che colpisce non solo le piccole Regioni, ma anche i piccoli partiti i quali non riuscirebbero a superare la soglia di sbarramento implicita per poter entrare in Parlamento andandone a compromettere la rappresentatività con la conseguenza di un possibile rischio della nascita di movimenti extraparlamentari che sono in grado di dare vita a situazioni di instabilità[347] che potrebbero comportare anche ad una crisi di Governo e ad elezioni anticipate. L'ulteriore ragione che ha giustificato tale riforma, poi, è stato il risparmio di spesa. Verrebbero risparmiati, secondo le stime, 500 milioni di euro a Legislatura, ma a fronte di una spesa annua di 4 miliardi[348] è una cifra alquanto irrisoria. Per cercare di porre rimedio alla crisi della democrazia rappresentativa vi era stata, inoltre, la proposta di estendere il diritto al voto ai sedicenni. Proposta che è naufragata per una serie di ragioni. In primis, se fosse stata approvata si sarebbe dovuto modificare l'articolo 2 del Codice civile, il quale statuisce che il raggiungimento della maggiore età, e di conseguenza della capacità di agire, è a diciotto anni. Si avrebbe dovuto, inoltre, modificare l'articolo 48 della Costituzione, il quale al co.1 statuisce "*Sono elettori tutti i cittadini, uomini e donne, che hanno raggiunto la maggiore età".* Oltre ad una ragione di carattere giuridico dovuta alla modifica della Costituzione e del Codice civile, vi è anche una ragione di carattere morale. È difficile sostenere che il minorenne sia in grado di sviluppare un'intelligenza politica, di valutare i programmi elettorali e comprendere l'importanza e la portata del diritto al voto. Non sarebbe in grado, in sostanza, di esercitare tale diritto in modo coscienzioso. A tale argomento si può facilmente obiettare che anche gli elettori spesso non maturano un'intelligenza politica ai fini di esercitare il diritto al voto coscientemente. L'età, dunque, non sarebbe un ostacolo per l'estensione di tale diritto. Tale proposta, poi, aveva alla base un ulteriore ragione, forse la principale, per contrastare la crisi della democrazia rappresentativa ossia con l'estensione del diritto al voto si avrebbe un ampliamento del corpo elettorale e un avvicinamento dei giovani alla politica. Tale risultato potrebbe essere anche raggiunto, ma non è detto che si realizzi in concreto.

Alla luce di queste riflessioni si può constare come difficilmente la crisi della democrazia rappresentativa possa essere ad oggi superata nonostante vi siano stati dei tentativi in tal senso. L'utilizzazione dei social e dei nuovi mezzi di comunicazione è ormai un dato evidente. Il caveat che è opportuno effettuare è il seguente: vi deve essere un uso attento da parte del corpo politico dei nuovi mezzi di comunicazione, il quale non deve sfruttare questi strumenti con lo scopo di strumentalizzarli e diffondere notizie false a danno degli avversari politici. Un uso attento che si raccomanda anche al corpo elettorale, il quale deve essere in grado di discernere le fake news e di informarsi adeguatamente. La strada da perseguire, dunque, non è quella di ricercare ossessivamente la formula elettorale perfetta

[347] *Ibidem*

[348] Si consulti per ulteriori informazioni https://pagellapolitica.it/articoli/costi-politica-parlamento-governo-ministeri

passando da un sistema maggioritario a uno proporzionale a uno misto che sia in grado di garantire un elevato livello di rappresentanza. Più che intervenire sulla rappresentanza, sarebbe opportuno fronteggiare il problema dell'astensionismo e cercare di riconquistare l'elettorato affinché possa nuovamente identificarsi e sentirsi rappresentato a tutti gli effetti dal corpo politico.

2.2. Internet Revolution e i nuovi mezzi di comunicazione

Nel precedente paragrafo si è analizzata la prima ragione per cui si discute di democrazia elettronica, ossia la crisi della democrazia rappresentativa e dei partiti politici causata da una pluralità di fattori, tra cui mutamenti del tessuto sociale, eventi storici e lo sviluppo tecnologico che ha indotto profondi cambiamenti nella relazione tra corpo elettorale e corpo politico. Si è cercato di individuare il rimedio più adatto a questa situazione di perenne crisi e si è osservato come il punto nevralgico su cui intervenire sia l'astensionismo per cercare di riaffezionare l'elettorato alla classe politica e favorire una maggior partecipazione elettorale. Si è constatato, inoltre, il ruolo fondamentale che la tecnologia ha nei processi democratici e del suo forte impatto nella relazione tra elettorato e rappresentante politico. Il tema di questo paragrafo, dunque, si concentra sugli effetti delle ICT e della tecnologia applicate ai processi decisionali, colonna portante della definizione stessa di *e-democracy,* andando ad analizzare, in particolare, i fenomeni delle bolle di filtro e delle camere di eco.

2.2.1. Le *filter bubbles*

È superfluo affermare che la tecnologia rappresenti, ad oggi, una componente essenziale nella vita dell'uomo contemporaneo. Internet, originariamente nato con uno scopo militare[349], è ormai onnipresente e la sua presenza non è esclusa nell'ambito dei processi decisionali coinvolgenti l'elettorato. L'utilizzo delle ICT in tali processi è la ragione che giustifica lo studio degli effetti della tecnologia nelle procedure democratiche da un punto di vista sociologico andando, dunque, a valutare l'impatto di queste tecnologie sulla democrazia. I fenomeni maggiormente conosciuti e discussi sono le *filter bubbles,* la cui evoluzione nella prospettiva della dinamica di gruppo consta nelle cc.dd. *echo chambers* e il sorgere dei movimenti populisti. Sono concetti di formulazione piuttosto recente, nati in concomitanza di Internet e della diffusione dei nuovi, quanto meno all'epoca, mezzi di comunicazione. Si tratta di fenomeni strettamente correlati alla democrazia elettronica, in quanto essa si fonda sulla

[349] Nel 1963 Joseph Licklider progettò l'Intergalatic Computer Network, ossia una rete di comunicazione per la quale chiunque utilizzando un computer sarebbe stato in grado di compiere qualsiasi tipo di operazione. Nel 1969 questo progetto venne finanziato per collegare in rete i centri di calcolo di quattro università americane impegnate nella ricerca in ambito militare e civile. Solo negli anni '90 Internet cambiò natura e divenne anche ad uso civile con la nascita al CERN del World Wide Web, ossia una rete utilizzata dagli impiegati del CERN per la condivisione di documenti grazie al collegamento ipertestuale http. Si veda Mazzola XVI, 2019.

comunicazione politica in Rete, per cui è necessario comprenderne non solo i risvolti positivi, ma anche i lati oscuri. Se all'inizio vi era una visione utopistica di Internet, considerato come un potente mezzo in grado di mettere in contatto più persone contemporaneamente e un luogo in cui poter liberamente manifestare le proprie idee e confrontarsi nell'agorà digitale con le opinioni altrui, con il passare del tempo è maturata la consapevolezza dei lati negativi delle Rete e della comunicazione digitale nella sfera pubblica. Eli Pariser, attivista politico e autore statunitense, partendo da queste riflessioni nel 2011 ha coniato l'espressione *filter bubbles,* ossia bolle di filtro. È una metafora utilizzata per descrivere la personalizzazione dei contenuti in Rete effettuata dalle piattaforme digitali, per cui le bolle di filtro rappresentano "*un universo di informazioni unico per ognuno di noi che dipende da chi siamo e da che cosa facciamo in Rete"*[350]. Questo universo unico nel suo genere è frutto della combinazione di una serie di elementi, ossia l'utilizzo di appositi filtri forniti dai principali motori di ricerca e dalle piattaforme social che consentono una ricerca personalizzata dei contenuti, la produzione di enormi quantità di dati da parte dell'utente e l'utilizzo di algoritmi di personalizzazione, ossia algoritmi che raccolgono i dati prodotti dall'utente rielaborandoli e presentandogli prodotti che potrebbero piacergli in base alle preferenze espresse in precedenza. Ad esempio, le piattaforme che forniscono servizi streaming utilizzano tali algoritmi per consigliare titoli che potrebbero piacere in base ai contenuti già visti. Il ragionamento alla base è il seguente: *ti è piaciuto questo, allora ti piacerà sicuramente quest'altro.* Il fulcro di questo fenomeno, dunque, consiste nell'utilizzo di algoritmi che sono in grado di prevedere quale sia il contenuto più adeguato da mostrare e quale, invece, sia da escludere in quanto non corrispondente alla preferenze espresse dall'utente. Si potrebbe affermare come le *filter bubbles* siano molto vicine alla profilazione, ossia meccanismo per il quale vi è una raccolta e un processamento dei dati personali con lo scopo di prevedere il verificarsi di determinati pattern e prende le decisioni *migliori* al momento *migliore.* In realtà, non vi è molto in comune in quanto si tratta di due concetti differenti tra loro. La profilazione, infatti, è la tecnica attraverso la quale si realizzano le *filter bubbles* ed è ciò che permette alle piattaforme digitali di guadagnare in termini monetari. Il guadagno, infatti, deriva dalla raccolta ed elaborazione dei dati forniti dall'utente che fungono, per così dire, da impronte digitali nel mondo del web. Più tempo viene trascorso sulla piattaforma, più dati vengono prodotti consentendo la creazione di un profilo *ad hoc* partendo dai *likes,* commenti, ricerche ed interazioni effettuate in Rete. Per ottenere più dati possibili, le piattaforme online utilizzano svariati stratagemmi, tra cui la tecnica dello *stickiness* per la quale i social presentano un design che favorisce una permanenza maggiore sfruttando, ad esempio, la psicologia dei colori[351],

[350] Pariser, Ted Talk.
[351] Ad esempio, Facebook ha come colore dominante il blu. Nella psicologia dei colori il blu rappresenta pace e tranquillità ed è il colore delle relazioni rappresentando rapporti sociali stabili.

un'interfaccia user friendly, ma anche novità e aggiornamenti che rendono la piattaforma più accattivante[352]. La profilazione, dunque, è evocativa delle *filter bubbles* che ne rappresentano la fattispecie patologica e il risultato di tale operazione. Si tratta, inoltre, di un fenomeno invisibile di cui l'utente non ne è a conoscenza e non comprende perché la ricerca di una determinata parola in Rete porta a risultati diversi rispetto a quelli di un'altra persona. In poche parole è un'operazione subdola che avviene all'insaputa dell'utente, il quale inconsciamente si trova chiuso in una bolla. Ed è questo particolare che rende le *filter bubbles* pericolose per la democrazia sotto diversi punti di vista. Ipoteticamente, se ognuno di noi fosse confinato in una bolla informativa, come anticipato da Negroponte nel 1995[353], verrebbe compromesso il principio del pluralismo, colonna portante della democrazia. Se non vi è la possibilità di un confronto tra maggioranza e opposizione, allora non si può parlare di democrazia che significa prendere una decisione che accontenti i più e che dia la possibilità alla minoranza di opporsi. L'effetto pregiudizievole delle bolle di filtro, pertanto, consiste nell'isolamento del singolo che comporta al rafforzamento del cc.dd. *confirmation bias*, ossia del pregiudizio di conferma il quale rappresenta la tendenza cognitiva dell'individuo a ricercare informazioni che confermino le sue convinzioni trascurando, invece, le informazioni che le potrebbero mettere in discussione. È da ricordare come le *filter bubbles* riguardino la dinamica del singolo, mentre su scala più vasta tale fenomeno prende il nome di *echo chambers,* ossia di camere di risonanza, per cui l'individuo interagisce preferibilmente con soggetti che condividono lo stesso punto di vista andandone a rafforzare e confermare le convinzioni preesistenti. Il problema sottostante alle bolle di filtro non riguarda solamente una limitata esposizione delle informazioni ricercate in Rete e il conseguente isolamento, ma anche il fatto che si tratta di un fenomeno invisibile e per tal ragione, dunque, può essere considerato come un qualcosa di sinistro. L'utente, difatti, non è consapevole di ciò che sta accadendo, ossia nel momento in cui naviga in rete i suoi dati vengono raccolti ed elaborati da parte degli algoritmi di personalizzazione che gli consegneranno un prodotto che potrebbe apprezzare poiché in linea con le preferenze espresse. Nonostante la presenza di questi rischi, negli ultimi anni si è cercato di dimostrare come la metafora delle *filter bubbles* abbia, in realtà, determinato un eccessivo allarmismo in materia di democrazia. In primis, il concetto stesso di *filter bubble* risulta essere poco chiaro, in quanto la definizione pecca di precisione. Si è osservato come la definizione di tale fenomeno sia un esempio pratico della dottrina del *Motte and Bailey* elaborata nel 2005 dal filosofo

[352] Ad esempio, Instagram da social di condivisione di fotografie nato, dunque, con una funzione di diario fotografico digitale si è trasformato nel corso degli anni in una piattaforma con molteplici funzionalità, tra cui la possibilità di condividere *stories,* ossia foto o brevi video della durata di ventiquattrore o *reels,* ossia brevi video con sottofondo musicale ispirati a TikTok.

[353] Nicholas Negroponte nel 1995 presentò il DailyMe, ossia un quotidiano online personalizzato in base alle preferenze espresse dagli utenti.

Nicholas Shackel. Tale dottrina consiste in una tecnica retorica per cui un soggetto statuisce un'affermazione controversa utilizzando termini vaghi implicanti conseguenze alquanto ambigue. L'affermazione di partenza è il *Bailey.* Nel momento in cui il *Bailey* viene contestato, esso viene riformulato in termini diversi dando vita ad un'affermazione meno controversa e più facilmente difensibile. Il *Bailey* rielaborato è il *Motte.* Una volta che il *Motte* è stato difeso, si torna all'affermazione di partenza[354]. In questa circostanza, dunque, il *Bailey* sarebbe rappresentato dai rischi dell'utilizzo della tecnologia nei processi democratici, mentre il *Motte* sarebbe rappresentato dalla realtà empirica delle *filter bubbles,* ossia due utenti non avranno mai lo stesso *feed* di ricerca, ma avranno risultati diversi. Vi è, poi, da considerare il fatto che è nella natura dell'uomo effettuare a priori una selezione dei contenuti a cui intende essere esposto ricercando informazioni che siano a supporto delle convinzioni in cui si crede. L'uomo per natura, infatti, evita il conflitto. Il fenomeno del *confirmation bias,* dunque non sarebbe un qualcosa di nuovo strettamente correlato con le *filter bubbles.* La presenza di questo fenomeno dal punto di vista sociale non è un qualcosa di recente, poiché anche nei secoli passati vi erano delle bolle di filtraggio, seppur in maniera diversa. Prendendo in considerazione, a titolo di esempio, la fine tra il XVIII e XIX secolo il principale mezzo di diffusione era la stampa e, poi, a partire dai primi del '900 la radio. Si può ritenere che anche all'epoca fossero presenti le bolle di filtraggio, in quanto non è un mistero il fatto che i borghesi e i notabili leggessero determinate testate giornalistiche e si radunassero nei salotti della città per discutere gli argomenti trattati dalla stampa. La classe operaia, invece, si riuniva presso luoghi comuni come le fabbriche per discutere vari temi, come la riduzione dell'orario di lavoro o un adeguato salario. Tra queste classi sociali, dunque, vi era una barriera costituita dal censo e dalle tematiche a cui si era esposti. Ad oggi, questo fenomeno è amplificato grazie ai social network e ai motori di ricerca. Rispetto al passato, però, è più agevole rompere la bolla, in quanto la dieta social dell'uomo contemporaneo è varia, pertanto gli viene data la possibilità di confrontarsi e attingere a fonti diverse che potrebbero mettere in discussione le sue certezze. L'utilizzo dei social media, dunque, non deve essere demonizzato, ma anzi incentivato in quanto consente un confronto continuo tra posizioni diverse. A fronte delle problematiche poste dalle *filter bubbles* è doveroso aprire una riflessione, seppur breve, sui possibili rimedi per evitare di consumare qualcosa che non sia stato creato appositamente per noi[355]. Il primo rimedio è semplice quanto banale, ossia l'educazione digitale dell'utente, il quale deve essere messo nelle condizioni di poter effettuare delle ricerche mirate che portino ad un determinato risultato e che allo stesso tempo sia in grado di riconoscere la presenza di una bolla di filtro e di farla scoppiare. Il secondo rimedio,

[354] Dahlgren, 2021
[355] Parafrasando la citazione di Eric Schmidt, CEO di Google tratta dal Ted Talk di Eli Pariser.

invece, riguarda la tecnologia. Sarebbe, infatti, prospettabile la creazione e lo sviluppo di algoritmi di personalizzazione che facciano emergere nelle ricerche non solo i risultati che siano più confacenti alle preferenze espresse dall'utente, ma anche risultati contrari alla tesi sostenuta. Vi è, però, un caveat: gli algoritmi non sono mai neutri, in quanto vengono programmati da esseri umani i quali potrebbero trasferire sull'algoritmo così creato i propri *bias,* ossia pregiudizi. Vi è, poi, da considerare l'intervento del Legislatore in materia. È difficile che il diritto stia al passo della tecnologia, poiché essa è in continuo sviluppo, ma non si deve escludere la possibilità di emanare delle linee guida, quindi *soft law*, per i provider Internet e le piattaforme digitali sulla trasparenza, sugli algoritmi utilizzati dal sistema e come vengono trattati e utilizzati i dati raccolti. Se per un verso vi è la necessità di un intervento da parte delle autorità competenti, dall'altro anche l'utente nel suo piccolo può agire per evitare di cadere nella trappola delle bolle di filtraggio. Quando si naviga in Internet vi sono i cc.dd. cookies[356] che raccolgono i dati di navigazione. Un primo rimedio, dunque, sarebbe quello di non accettare i cookies di profilazione per ridurre l'apporto di dati raccolti e la loro rielaborazione. In questo modo vengono ridotte le possibilità di essere sottoposti a profilazione e di ottenere risultati di ricerca simili alle preferenze precedentemente espresse e rintracciate dagli algoritmi di personalizzazione. L'utente, poi, potrebbe sfruttare i social a proprio favore seguendo personaggi, notiziari etc. che non sono in linea con le sue idee, ma che rappresentano un'opportunità per poter venire a contatto con idee diverse e rompere la bolla di filtro in cui rischia di essere rinchiuso. Sono delle piccole accortezze che potrebbero far la differenza se adottate da ognuno di noi. Come si suol dire l'unione fa la forza, perciò più utenti in Rete si impegnano ad evitare di essere confinati nelle loro bolle e nelle camere di risonanza, più vi è la possibilità di successo di contrastare questi fenomeni. Le soluzioni così prospettate, però, scontano un limite. La creazione di speciali algoritmi che consentano l'esposizione dell'utente a contenuti diversi da quelli a cui sarebbe normalmente esposto, nonché il rifiuto dei cookies che raccolgono i dati di navigazione sono tutte soluzioni strettamente dipendenti dalle piattaforme digitali, pertanto risulta piuttosto difficile arginare tale fenomeno. Considerato, poi, in che cosa consistono le *filter bubbles* è rilevante osservare come si tratti nella sostanza di una limitazione circa la circolazione delle idee non prevista dai termini e dalle condizioni d'uso[357]. In

[356] I cookies sono dei file di testo necessari affinché il server del sito web possa ottenere informazioni sull'attività che l'utente compie sul sito. I cookies si suddividono in (i) tecnici, ossia sono quelli che consentono il corretto funzionamento del sito web, (ii) analitici, ossia hanno la funzione di fornire al gestore della piattaforma dati statistici ed infine (iii) di profilazione utilizzati per la raccolta dei dati lasciati dall'utente durante la permanenza sul sito web e creare un profilo *ah hoc* per scopi commerciali attraverso l'invio di messaggi pubblicitari. Si consulti https://www.agendadigitale.eu/infrastrutture/tutto-quello-che-dobbiamo-sapere-sui-cookie-per-la-privacy-da-utenti-o-gestori/

[357] Si sono considerati, come esempi, le condizioni d'uso dei social Instagram e X, in quanto maggiormente diffusi e utilizzati. È notevole la differenza nel tenore dei testi. Per quanto riguarda Instagram, vi sono continui rinvii a collegamenti ipertestuali esterni per ottenere ulteriori informazioni. È interessante osservare come il linguaggio sia particolarmente

conclusione, si può affermare come nonostante sia diffuso il fenomeno delle bolle di filtro ciò non deve destare un allarmismo eccessivo, poiché si è dotati di tutti gli strumenti necessari per poterlo contrastare. Strumenti che, a volte, vengono forniti dalle piattaforme stesse ma la cui efficacia è alquanto dubbia[358]. Al momento, dunque, sono presenti pochi rimedi per cercare di arginare le *filter bubbles,* nonostante questo sono dei primi passi verso la rottura della bolla virtuale in cui ogni utente online si trova involontariamente confinato.

2.2.2. Le *echo chambers*

La dieta social prevede per ogni utente contenuti diversi altamente personalizzati e adeguati alle esigenze del singolo. Ogni utente, dunque, è chiuso nella propria bolla di filtraggio che difficilmente riuscirà a far scoppiare. L'uomo, però, è un animale sociale e Internet ha dato e dà la possibilità di instaurare rapporti con altri attraverso le piattaforme social, i blog e i forum. Nel momento in cui si interagisce online con altri attraverso commenti, condivisioni e messaggistica istantanea è naturale rendersi conto di seguire quella determinata persona perché se ne condividono le idee e perché se ne apprezzano i contenuti, in quanto sono coerenti con le proprie convinzioni e ideologie. Questa dinamica non è ristretta ad un solo utente, ma ad una pluralità di soggetti e ciò porta alla creazione delle cc.dd. *echo chambers* o camere d'eco, dette altrimenti casse di risonanza. È una metafora coniata da Cass Sunstein per descrivere quel fenomeno, considerato come un'evoluzione delle *filter bubbles,* per il quale un gruppo di soggetti interagisce tra di loro condividendo le stesse opinioni, visioni, ideologie creando un ciclo di conferma e amplificazione delle proprie prospettive rifiutando, invece, critiche o opinioni divergenti, le quali vengono per lo più ignorate o considerate come esempi da non

accomodante nei confronti dell'utente mettendolo al centro. Ad esempio, nella sezione dedicata ai servizi di Instagram viene asserito *"Sviluppiamo sistemi per provare a comprendere chi e cosa sia di interesse per l'utente […] e usiamo tali informazioni per aiutare l'utente a creare, trovare, partecipare e condividere esperienze rilevanti"* o ancora "*In base alle scelte e alle impostazioni selezionate dall'utente, usiamo le informazioni di Instagram e di altri prodotti delle aziende di Meta […] per personalizzare l'esperienza dell'utente su Instagram, ad esempio mostrando inserzioni offerte e altri contenuti sponsorizzati che riteniamo possano essere di suo interesse".* X, invece, a differenza di Instagram non mette al centro l'utente. Nei termini di servizio, infatti, è previsto solamente che l'utente è responsabile dei contenuti postati. Tali contenuti possono essere usati, copiati, riprodotti, trattati, pubblicati e distribuiti "*in qualsiasi tipo di supporto o sistemi di distribuzione, noti ora o sviluppati in futuro".* La piattaforma di Elon Musk sembra non interessarsi molto dell'utente se non per poterne usufruire i contenuti. Per ulteriori approfondimenti si veda: https://help.instagram.com/581066165581870, https://transparency.meta.com/features/explaining-ranking/ e https://x.com/it/tos.

[358] Mi riferisco alla recente comunicazione da parte di Meta agli utenti circa l'utilizzo dei contenuti postati sulle sue piattaforme Instagram e Facebook per il training di Meta AI affinché possa produrre contenuti a sua volta. È possibile esercitare il proprio diritto di opposizione fino al 26 giugno. Ciò che emerge è il seguente rilievo critico, ossia si tratta sì di una comunicazione ufficiale, ma inviata tramite e-mail la quale risulta essere poco efficace, poiché l'utente medio non vi presta, generalmente, molta attenzione. Non a caso, nei giorni in cui questa comunicazione è stata resa nota sono stati diffusi vari *templates* su Instagram su come presentare opposizione. Nonostante il diritto di opposizione dell'utente sia presente, nulla garantisce che la propria richiesta venga *effettivamente* presa in carico da Meta, pertanto vi è sempre il rischio che i propri contenuti possano essere sfruttati per l'addestramento dell'intelligenza artificiale.

seguire. Nonostante sia un concetto conosciuto e studiato da diverso tempo, ad oggi non è ancora presente una definizione del tutto univoca di *echo chambers,* in quanto è un fenomeno che colpisce vari aspetti della vita umana. In primo luogo, l'uomo è un animale sociale quindi nell'approfondimento di questo fenomeno è coinvolto l'aspetto delle relazioni interpersonali. Le camere di eco, infatti, vengono studiate in sociologia focalizzandosi sui modelli di comportamento sociali e sulla presenza di eventuali pattern che comportano al loro verificarsi e il loro impatto nella società andandone ad indagare i fattori scatenanti. Le camere di eco, poi, non riguardano solo le relazioni umane, ma anche la psiche, dunque, lo studio delle *echo chambers* si concentra anche sull'aspetto piscologico esplorando come il singolo interagisce con l'ambiente che lo circonda e con altri individui indagandone i processi mentali e il comportamento. Nell'ambito delle *echo chambers* si presta attenzione al fattore emotivo, poiché le emozioni, soprattutto quelle negative, sono un collante sociale e dunque risultano particolarmente rilevanti in tale contesto, nel quale si condividono opinioni simili rafforzando l'identità di gruppo e andando, in un certo senso, ad annullare la propria. Infine, le camere di eco coinvolgono anche il settore tecnologico in quanto si sviluppano in Rete e sfruttano a loro favore, condividendo questo aspetto con le bolle di filtro, gli algoritmi di personalizzazione e il meccanismo della profilazione allo scopo di fornire contenuti che siano lo specchio delle preferenze espresse dall'utente online. Non si riscontrano, dunque, molte differenze dal punto di vista concettuale rispetto alle *filter bubbles,* in quanto le camere di eco ne sono uno sviluppo in una dimensione più ampia. Le bolle di filtro, infatti, riguardano la dinamica del singolo, mentre il fenomeno in analisi concerne la dinamica di gruppo. Dal punto di vista degli effetti, empiricamente parlando, si riscontra qualche differenza rispetto alle *filter bubbles.* Le camere di eco, infatti, essendo un fenomeno attinente alla dinamica di gruppo concretizzano ciò che è stato individuato da Solomon Asch negli anni '50 del secolo scorso, ossia l'effetto conformativo. È interessante l'esperimento condotto dallo psicologo polacco, in quanto ha dimostrato come un individuo inserito in un gruppo tende a conformarsi ad esso dando una risposta errata al quesito posto[359] onde evitare di essere considerato diverso o di esporsi ad un eventuale giudizio negativo[360], pur essendo consapevole che la risposta data non sia quella corretta. Tale effetto conformativo si verifica anche nelle camere di eco, in quanto più un'idea circola e si diffonde tra gli appartenenti al gruppo, più essa si consolida e dunque, anche se alcuni sono consapevoli della sua assurdità o ne vorrebbero contestare il fondamento, non riescono perché, altrimenti, si esporrebbero

[359] L'esperimento in questione consisteva nell'individuare a quale delle tre linee indicate corrispondesse in lunghezza quella mostrata come riferimento. Il gruppo era costituito da otto individui, di cui sette istruiti a fare la risposta errata, ma univoca; mentre l'ottavo soggetto era colui che veniva sottoposto all'esperimento.
[360] Sarra, 2022

ad una disapprovazione da parte del gruppo con il rischio di essere *bannati*[361] da esso. L'idea, l'opinione o la teoria che circola all'interno della *echo chamber* si consolida cambiando leggermente forma, mantenendone, però, la sostanza. Detto altrimenti, il concetto alla base è lo stesso, ma le parole o il modo con cui viene espresso cambiano di poco. Ulteriore conseguenza di tale dinamica è il rifiuto di interagire con altri soggetti che potrebbero sostenere argomenti che metterebbero in crisi, o quantomeno, in dubbio il credo di gruppo. Il meccanismo, dunque, che si innesta all'interno delle *echo chambers* è una forma di discriminazione per la quale il diverso non viene accettato. Il consolidamento dell'identità di gruppo e il rafforzamento delle idee condivise dagli appartenenti ad esso che, involontariamente o non, si trovano chiusi in una cassa di risonanza ha come risultato non solo il rifiuto di esporsi e accettare il diverso, ma anche l'estremizzare le teorie condivise che si possono tradurre in due fenomeni, ossia la polarizzazione e, conseguentemente, l'emersione e la diffusione delle cc.dd. teorie del complotto. Per quanto riguarda la polarizzazione, essa consiste nella tendenza di un individuo a sostenere con fermezza una determinata posizione. Nel linguaggio politico si traduce nell'inclinazione dell'elettorato "*a concentrare i suffragi su due partiti o gruppi di partiti tra loro contrapposti"*[362]. A titolo esemplificativo, si tratta di quella circostanza per la quale una parte dell'elettorato sostiene il partito A di destra e una parte dell'elettorato sostiene, invece, il partito B di sinistra. Si registra, dunque, una divergenza nelle posizioni politiche verso estremi ideologici[363] che innalza notevolmente il rischio di una spaccatura all'interno del contesto politico con l'eventualità di sviluppare e farsi portatori di idee radicali[364]. La polarizzazione, poi, provoca, se a livelli elevati, intolleranza, cinismo politico e ridotte opportunità di collaborazione e compromesso[365]. Tutto ciò mette a rischio la democrazia, in quanto non vi sarebbe un margine di discussione per giungere alla soluzione *migliore* che accontenti la maggioranza e verrebbe meno il valore principe, ossia il

[361] Nel linguaggio del web essere *bannati* significa essere esclusi dal gruppo. È un'arma difensiva che viene utilizzata dai moderatori, in quanto il diretto interessato potrebbe aver condiviso opinioni contrarie al regolamento previsto o essersi espresso con termini offensivi verso altri componenti. Il *ban* può essere temporaneo o permanente.
[362] Enciclopedia Treccani, voce polarizzazione.
[363] Alatawi, et al., 2021
[364] Si può fare un paragone, seppur azzardato, con le dittature del primo '900. Si può, in un certo senso, affermare come anche in quel particolare periodo storico connotato da due guerre mondiali e dall'ascesa del nazionalsocialismo vi fossero delle *echo chambers* di prima generazione. Se si confronta il passato con il presente ci si rende conto di come non siano presenti molte differenze. In primis anche se non vi era ancora Internet, i principali mezzi di comunicazione di massa erano la stampa e i giornali e non si può escludere, poi, che come oggi circolano nel web le cc.dd. *fake news,* anche all'epoca vi fossero traccia nei media di massa di notizie false diffuse a sostegno della propaganda elettorale ai fini del consolidamento del regime. Da ciò deriva, in secondo luogo, l'assenza di pluralismo sia di partito che di fonti a cui attingere. Dal momento che, in maniera legittima tramite regolari elezioni o a mezzo di *Coup d'État*, si era affermato un solo partito, ciò ha comportato, poi, al consolidarsi di un solo credo considerato quello *giusto* da seguire, per cui non si ammettevano opinioni contrastanti. Se, ad oggi, la punizione per il dissidente è quella di essere *bannato* dal gruppo o dalla piattaforma social, all'epoca i mezzi di contrasto erano ben diversi e più forti. In passato, probabilmente, non vi era la consapevolezza che, invece, c'è oggi circa la presenza delle *echo chambers,* anche se vi è ancora una certa difficoltà nell'individuare tale fenomeno e nel darvi una definizione univoca.
[365] Hobolt , Lawall , & Tilley, 2023

pluralismo. È indubbio, dunque, che nelle *echo chambers* vi sia un elevato rischio di polarizzazione porta alla proliferazione di idee estreme, le quali a loro volta si possono trasformare nelle cc.dd. teorie del complotto. In generale, una teoria complottista può essere riassunta nel motto *ci stanno nascondendo la verità,* ossia i sostenitori di tali teorie ritengono che chi è al potere stia nascondendo la verità al popolo senza condividere il proprio sapere con la gente comune. È compito, dunque, dell'uomo comune farsi portatore di una causa contro i poteri forti e a tal fine elabora una propria teoria a contrasto. Questo effetto delle *echo chambers* è particolarmente pericoloso, in quanto è un fenomeno che si diffonde velocemente, soprattutto con la presenza di Internet e dei social, principali veicoli di tali teorie e soprattutto perché in alcuni casi anche i Governi tendono a credervi[366]. Ulteriore conseguenza della polarizzazione e della diffusione di teorie del complotto è la disinformazione. Per disinformazione si intendono tutte le forme di informazioni che sono false, inaccurate o fuorvianti confezionate *ad hoc* per far leva su una determinata fetta di pubblico ai fini di cagionare danni o per trarne profitto[367]. A titolo di esempio, vi sono i cc.dd. titoli *clickbait,* ossia titoli volutamente fuorvianti che inducono il lettore incuriosito a cliccarci sopra e ad aprire la pagina web[368]. La diffusione di notizie false all'interno delle *echo chambers* avviene principalmente attraverso due processi, ossa il *seeding* e l'*echoing*[369]. Per quanto riguarda il *seeding,* che nel linguaggio di Internet significa inizializzazione, è la fase in cui vi è la diffusione di una narrativa controcorrente caratterizzata da informazioni prive di fonti e decontestualizzate con l'obiettivo di influenzare le opinioni altrui[370]. Durante la pandemia da COVID-19 è noto che vi è stata la diffusione di molte notizie, rivelatesi per lo più false, sull'origine del virus e sugli effetti collaterali dei vaccini[371] agli inizi della diffusione della malattia e della sperimentazione medica. Una volta che le informazioni si sono diffuse tra il pubblico e, dunque, si sono consolidate si passa alla fase successiva, ossia l'*echoing* meccanismo attraverso il quale la disinformazione viene disseminata nelle casse di risonanza sfruttando controversie preesistenti su un determinato argomento andando a contrastare narrative alternative con la propria[372]. Ciò che emerge, quindi, è la presenza di utenti attivi consumatori di informazioni online, le quali vengono diffuse nel loro *network* sfruttando i canali social andando, così, a rafforzare la narrativa sostenuta dal gruppo di

[366] Un esempio della pericolosità di tale fenomeno è il Governo del Sud Africa che tra gli anni '90 e gli inizi degli anni 2000 ha ignorato la diffusione dell'HIV e dell'AIDS causando la morte di circa centomila persone all'anno. Si consulti https://www.saluteinternazionale.info/2016/07/big-pharma-una-storia-che-si-ripete/
[367] Diaz Ruiz & Nilsson , 2023
[368] Questa è una delle tante tattiche che viene utilizzata per ottenere dati sugli utenti ai fini della profilazione, oltre che di guadagno.
[369] Dubois & Black, 2018
[370] Diaz Ruiz & Nilsson , 2023
[371] A titolo esemplificativo, il Ministero della Salute, durante la pandemia, ha dedicato un'apposita pagina sulle notizie false maggiormente diffuse sul COVID-19 smentendole in base alle evidenze disponibili. Si veda https://www.salute.gov.it/portale/nuovocoronavirus/archivioFakeNewsNuovoCoronavirus.jsp
[372] *Ibidem*

appartenenza. Ci si trova però in un paradosso, l'ennesimo di questo fenomeno. Si è propensi a ritenere che più social vengono utilizzati dall'utente medio, più egli ha la possibilità di esporsi a diverse opinioni politiche e notizie, anche qualora non fosse interessato a questo genere di informazioni. Il *media diversity*, ed è qui che si insinua il paradosso, potrebbe avere un effetto boomerang, in quanto non è detto che il consumo di più prodotti sia la medicina migliore per contrastare le *echo chambers.* Difatti, le informazioni così assorbite dai diversi canali social potrebbero andare a rafforzare non solo l'identità di gruppo e l'effetto conformativo, ma anche quanto sostenuto nella *echo chamber* con il risultato di potenziare anche quello che è stato individuato poc'anzi nell'effetto della polarizzazione. Le *echo chambers,* inoltre, non riguardano solo la dinamica di gruppo e gli effetti che si producono a livello sociale poiché si tratta di un fenomeno che ha delle conseguenze anche dal punto di vista della democrazia e dei processi decisionali. Si è detto in precedenza come la polarizzazione, ossia il sostenere fermamente una determinata posizione, produca come effetti un aumento del cinismo politico, intolleranza e una ridotta opportunità di collaborazione per giungere ad un compromesso, essenziale in democrazia. Queste sono solo alcune delle ripercussioni delle camere di eco sulla democrazia. In primo luogo, appoggiando idee alquanto radicali vi è una visione cinica nei confronti della politica con una certa sfiducia nelle istituzioni e disprezzando i valori stessi della democrazia quali la libertà, l'uguaglianza e il pluralismo. Sono tutti valori che potrebbero essere a rischio in presenza di *echo chambers* diffuse, in quanto il pluralismo verrebbe meno poiché si ritiene che la propria idea sia la *migliore* e dunque non vi è spazio per accettare opinioni diverse. Ciò comporta, dunque, ad una paura irrazionale per il diverso aumentando, di conseguenza, l'incidenza dei fenomeni discriminatori. Strettamente correlato a questo aspetto non vi è certezza circa la tenuta della libertà di espressione, la quale può essere, in un certo senso, limitata fino a sfociare in una possibile censura. Censura che può avvenire attraverso la moderazione dei contenuti all'interno del gruppo oppure attraverso il controllo delle parole ammesse e quelle vietate. Cinismo, intolleranza e mancanza di compromesso sono le maggiori minacce che potrebbero potenzialmente nuocere alla democrazia. Non solo la democrazia come tradizionalmente intesa è sotto attacco, ma anche l'*e-democracy* non risulta essere esente da questi pericoli. La Rete, infatti, è la culla della democrazia elettronica e nell'immaginario di questa teoria viene rappresentata come il luogo in cui avviene lo scambio di idee e opinioni come in una sorta di agorà digitale. Il dibattito politico, quindi, viene incentivato in una dimensione non tangibile giungendo alla disintermediazione e attivando strumenti di democrazia diretta come i referendum. La presenza, però, di bolle di filtraggio e di *echo chambers* minaccia il dibattito politico online facendo sì che venga meno l'essenza della democrazia elettronica come alternativa alla democrazia rappresentativa. In sostanza, dunque, le *echo chambers* e le *filter bubbles* minerebbero le fondamenta della democrazia elettronica, la quale non sarebbe più un'alternativa alla

democrazia rappresentativa e, dunque, risulterebbe essere un concetto che cadrebbe nel vuoto. Vi sono, però, alcuni rimedi per cercare di arginare tali fenomeni e far sì che l'utente sia in grado di riconoscere se è chiuso o meno in una cassa di risonanza. Non sono molti e per lo più sono già quelli evidenziati con le *filter bubbles*, ossia l'educazione digitale del singolo, la disattivazione dei *cookies* e un intervento in materia da parte del legislatore. Un appunto che si vuole aggiungere riguarda l'aspetto dell'educazione dell'individuo. Dal punto di vista sociale, l'apertura di mente, intesa come l'esposizione a nuove idee e culture è tipica di chi ha un livello di educazione elevato[373]. Educazione che non deve essere intesa in senso stretto del termine, ossia il grado di istruzione, in quanto per educazione si intende il bagaglio culturale dell'individuo frutto non solo dell'istruzione ricevuta, ma anche degli hobbies, viaggi e tutto ciò che mette l'individuo in contatto con il mondo e lo fa approcciare a nuove esperienze. Questi elementi aiutano, dunque, a sviluppare un pensiero critico più profondo e di confrontarsi con idee diverse che potrebbero far vacillare il proprio credo. Ultimo, ma non per importanza, chi sostiene una posizione moderata o *mainstream* generalmente ha meno probabilità di essere vittima delle *filter bubbles* e delle *echo chambers* in quanto non sostiene una posizione radicale e quindi evita, con più facilità, la polarizzazione. In sintesi, i fenomeni delle bolle di filtro e delle camere di eco pur essendo presenti non devono destare troppo allarmismo. Sono evidenti i rischi che la democrazia corre vedendo minacciati i valori fondamentali quali pluralismo e libertà, ma è altrettanto evidente come ad oggi si è dotati di tutti gli strumenti necessari per poterli contrastare, a partire dal singolo che può con semplici accorgimenti può ridurre le probabilità di essere confinato in una bolla di filtraggio e in una camera di eco. Si hanno tutte le carte in tavola per combattere questi fenomeni per evitare irreparabili ripercussioni non solo dal punto di vista sociale, ma anche democratico. La strada da percorrere, però, è ancora lunga.

3. Il caso dell'Estonia

Non è stato difficile individuare il Paese pioniere nel campo della democrazia elettronica, in quanto è assai noto che gli Stati appartenenti all'ex blocco sovietico paradossalmente sono tra i più avanzati al mondo in materia di tecnologia e soluzioni di *e-governance* e di *e-democracy.* Paradossalmente, poiché fa "strano" in un certo senso pensare che paesi che solitamente vengono considerati poco all'avanguardia rispetto all'Europa Occidentale siano, in realtà, l'esatto contrario. L'Estonia è una dimostrazione di quanto asserito, in quanto è riuscita a sfruttare a proprio vantaggio la posizione di svantaggio in cui si trovava e a diventare l'unico paese al mondo ad utilizzare il voto online, ossia il

[373] Chan, Zhao , & San Lee , 2023

remote Internet voting[374]*,* in tutti i tipi di elezione, da quelle per il rinnovo del Parlamento locale alle elezioni del Parlamento Europeo[375]. Il *remote Internet voting* ha avuto successo in Estonia per una serie di fattori. In primis, il voto online non ha del tutto sostituito il voto tradizionale né si tratta di un sistema alternativo ad esso. Il RIV viene, infatti, individuato come uno strumento ulteriore, aggiuntivo attraverso il quale i cittadini possono esercitare il loro diritto al voto ed esprimere le proprie preferenze. In secondo luogo, tale sistema permetterebbe una partecipazione politica più attiva e un aumento del suffragio, in quanto si tratta di uno strumento che permette agli elettori di esprimere il proprio voto da qualsiasi device elettronico, purché sia collegato ad una rete Internet[376]. Ciò consente, dunque, di votare in qualsiasi momento e da qualsiasi luogo, senza la necessità di recarsi fisicamente alle urne. Ulteriori fattori che hanno contribuito al successo del *remote Internet voting* riguardano l'aspetto sociale, culturale e legislativo. Per quanto riguarda gli aspetti sociali e culturali, il popolo estone è stato fin da subito *abituato* all'innovazione e alla sperimentazione in materia di processi decisionali con la creazione, sviluppo ed implementazione della tecnologia nella politica. È presente, dunque, una cultura aperta all'innovazione favorita anche dal fatto che i primi esperimenti in materia sono avvenuti in piena Internet Revolution contribuendo, dunque, allo sviluppo delle infrastrutture e della diffusione dell'educazione digitale facendo sì che il problema del digital divide si ponesse in misura minore se confrontato con altri Paesi. Ulteriore elemento che ha contribuito a rendere l'Estonia un *e-State* è stato il periodo di recessione e di crisi economica che il Paese ha dovuto affrontare dopo la caduta della Cortina di ferro. La crisi, oltre ad essere la naturale conseguenza dell'improvviso cambiamento dello status quo ante, è risultata propizia per lo sviluppo dell'Estonia nel campo tecnologico e politico. La situazione di partenza, infatti, non era delle migliori, in quanto non era presente un adeguato sistema di infrastrutture e di telecomunicazioni tali per cui fosse possibile una diffusione capillare di Internet, ma ciò ha sortito l'effetto di un maggior coinvolgimento del settore pubblico a discapito di quello privato per l'implementazione e la diffusione di soluzioni tecnologicamente avanzate, nonché la liberalizzazione delle telecomunicazioni creando *liaison* con privati al fine di ottenere numerosi investimenti che permettessero il rilancio economico del Paese[377].

Osservando la cronologia degli eventi, nel 1994 vi è la stesura del testo *Principles of Estonian information policy*, ossia un documento in cui venivano stabilite le linee guida per lo sviluppo IT del Paese, ratificato dal Parlamento, poi, nel 1998[378]. Il primo tassello vero e proprio che ha portato allo

[374] Per brevità da ora in poi verrà indicato con l'acronimo RIV
[375] Sciannella, 2020
[376] Ehin, Solvak, Willemson, & Vinkel, 2022
[377] Scianella, 2015
[378] https://digiexpo.e-estonia.com/story-of-e-estonia/

sviluppo dell'*e-State* estone è la diffusione nel 1996 del progetto *Tiger Leap,* il quale si poneva tre obiettivi, ossia (i) la diffusione massificata dei computer e della rete Internet, (ii) una formazione di base per gli insegnati e (iii) materiale didattico elettronico in lingua madre per tutti gli istituti scolastici[379]. Si tratta, dunque, di un progetto diffuso nelle scuole di qualsiasi ordine e grado funzionale all'educazione digitale delle nuove generazioni e degli insegnanti al fine di evitare il più possibile il divario digitale e far sì che fin dalla tenera età si fosse a stretto contatto con il mondo *digital* alimentando, dunque, una cultura aperta all'innovazione e alla sperimentazione. A seguito del successo del progetto, negli anni successivi fu sviluppato il *Tiger Leap Plus* con l'obiettivo di migliorare le competenze tecniche di alunni ed insegnati attraverso la creazione di materiale educativo in formato digitale[380]. Vi furono, poi, ulteriori sviluppi a livello di digitalizzazione del Paese. A titolo di esempio, nel 2001venne creato *X-Road,* un enorme centro di scambio di informazioni tra più database con l'intento di integrare le varie piattaforme presenti a livello nazionale per ridurre i costi, aumentare l'efficienza e la sicurezza evitando così eventuali *data leak*[381]. Sicuramente una delle tappe più importanti è il 2005, anno in cui si è introdotto l'i-Voting consentendo l'esercizio del diritto al voto in forma elettronica su Internet attraverso qualsiasi dispositivo elettronico. Dal punto di vista legislativo, l'Estonia fin dagli inizi si è dotata in un adeguato apparato che regolamentasse tale fenomeno con la consapevolezza che il diritto difficilmente riesce a stare al passo dell'evoluzione tecnologica. Nel 2000 venne approvato il *Telecommunication Act*, il quale si pone come obiettivi la creazione di condizioni propizie per lo sviluppo delle telecomunicazioni e tutelare gli utenti attraverso la promozione della concorrenza libera[382]. La creazione di infrastrutture adeguate e lo sviluppo del settore tecnologico sono, infatti, le colonne portanti che sorreggono quello che è stato il percorso evolutivo che ha portato l'Estonia ad essere lo Stato leader in materia di votazione elettronica e rapporto con la cittadinanza. Nel 2002 venne approvato il *Local Government Council Election Act*, modificato poi nel 2005, anno in cui vi è stata l'introduzione del *remote Internet voting*. Tale testo regola il sistema elettorale andandone a disciplinare vari aspetti come chi può esercitare il diritto al voto[383], la campagna elettorale e la procedura di votazione. È un documento che disciplina ogni aspetto relativo all'esercizio del diritto al voto sia per quanto riguarda l'elettorato attivo sia per quanto riguarda l'elettorato passivo. Nel 2005

[379] https://www.educationestonia.org/tiger-leap/
[380] *Ibidem*
[381] https://e-estonia.com/story/
[382] §1 del Telecommunication Act (2000)
[383] In base a quanto previsto dal §5 i cittadini Estoni e i cittadini dell'Unione Europea che abbiano raggiunto di 18 anni al momento delle elezioni e coloro che risiedono in maniera permanente in Estonia hanno il diritto di votare. È curioso osservare che a differenza del sistema italiano, il quale prevede che solo i coloro dotati della cittadinanza italiana possono votare, in Estonia la cittadinanza non è un requisito essenziale per esercitare tale diritto. È sufficiente, infatti, essere cittadini dell'Unione Europea e risiedere in Estonia. Ciò comporta, evidentemente, ad un aumento della platea degli aventi diritto al voto con conseguente aumento della partecipazione elettorale.

il *Local Government Council Election Act* fu emendato a seguito dell'introduzione del *remote Internet voting* dando la possibilità agli elettori di modificare il voto online fino al giorno antecedente le elezioni ed eventualmente ripetere il voto in sede di seggio elettorale andando, dunque, ad annullare la preferenza espressa in via digitale. Si coglie, dunque, come sia una modalità di voto aggiuntiva a quella tradizionale senza avere la pretesa di andarlo a sostituire completamente consentendo all'elettore di rettificare la propria decisione in più occasioni. Il caso dell'Estonia insegna come sfruttare al meglio situazioni di disagio per diventare uno dei paesi più avanzati al mondo in termini di *e-governance* e di *e-democracy.*

3.1. Il *remote Internet voting*: introduzione

Il *remote Internet voting* non deve essere confuso con il voto elettronico, in quanto è una sua variante. I due concetti, infatti, non coincidono. Il Consiglio d'Europa traccia una linea di confine tra il RIV e il voto elettronico. Quest'ultimo viene definito come l'hardware, il software e il processo che consente agli elettori di votare attraverso strumenti digitali durante le elezioni o durante un referendum. Il voto online, invece, è caratterizzato dall'utilizzo di dispositivi elettronici per votare al di fuori dei luoghi tradizionali in cui la procedura prende atto, ossia i seggi elettorali[384]. Il voto elettronico, dunque, è l'architettura attraverso la quale è possibile esprimere le proprie preferenze, mentre il *remote Internet voting* è uno degli strumenti attraverso il quale è possibile esercitare il diritto al voto. Il punto di contatto tra il voto elettronico e l'i-Voting è l'utilizzo della tecnologia a supporto delle operazioni elettorali[385]. Si è portati a ritenere che votare attraverso piattaforme elettroniche o con modalità digitali sia una procedura che vada a semplificare il processo elettorale, ma il voto espresso attraverso queste modalità richiede una serie di accorgimenti che nella forma tradizionale non vengono presi in considerazione. In primo luogo è necessario sviluppare delle piattaforme che siano sufficientemente resilienti agli attacchi informatici onde evitare possibili problemi in materia di cybersicurezza con il rischio della diffusione dei dati personali di cittadini e residenti. Bisogna, però, considerare che non è possibile garantire un sistema che sia totalmente immune da aggressioni informatiche, in quanto il mondo hacker è in continua evoluzione ed è molto plausibile, anzi è certa, la creazione di nuovi malware o di nuove tecniche che consentono l'ingresso ai sistemi di sicurezza nazionali, malgrado questi vengano costantemente aggiornati con nuovi meccanismi di difesa. In secondo luogo è necessario compiere una scelta che risulta essere cruciale per il successo della modalità di votazione elettronica, ossia scegliere tra il voto elettronico presidiato e il voto elettronico non presidiato. Il voto

[384] Sciannella, 2020
[385] *Ibidem*

elettronico presidiato può essere considerato come una forma aggiuntiva al tradizionale voto alle urne o, in alternativa, come unica modalità di espressione del voto ed è "*reso dall'elettore in postazioni di voto sorvegliate da pubblici ufficiali"*[386]. Il voto elettronico non presidiato, come nel caso dell'Estonia, consente l'esercizio del diritto al voto tramite applicazioni o siti web a distanza in qualsiasi luogo, terminale e in assenza di un supervisore come un pubblico ufficiale[387]. La scelta tra la forma presidiata e non comporta a conseguenze di particolare rilievo circa l'opportunità di implementazione di tale procedura. Il voto presidiato può essere considerato come una sorta di aggiornamento della modalità tradizionale, in quanto ciò che cambia non è il recarsi fisicamente alle urne, ma lo strumento attraverso il quale per esercitare il proprio diritto al voto. Tra i principi afferenti al diritto al voto, quello della sicurezza viene sicuramente valorizzato al massimo, in quanto non vi è il rischio di possibili coercizioni esterne o manipolazioni da parte di terzi alla propria volontà essendo presidiato da un pubblico ufficiale. Di contro, però, il voto elettronico presidiato pur garantendo una certa sicurezza da coercizioni esterne, non assicura la comodità che il voto elettronico non presidiato, invece, fornisce. Il poter votare in qualsiasi momento, da qualsiasi dispositivo comporta ad una libertà assoluta nel poter esercitare tale diritto al prezzo, però, della segretezza del voto. Non è da escludere, infatti, che il voto nella forma non presidiata non sia immune da possibili influenze che facciano sì che l'elettore sia guidato ad esprimere una preferenza diversa dalla propria. Bisogna, dunque, scegliere se valorizzare la sicurezza o la libertà che si traduce in comodità e possibile maggiore affluenza. In terzo luogo, nello sviluppo di piattaforme di voto online è necessario considerare non solo l'aspetto della sicurezza, ma anche l'approccio con l'utente. Le piattaforme adibite a tale funzione, infatti, devono essere dotate di un'interfaccia che sia il più *user friendly* possibile sotto diversi aspetti. Dal punto di vista meramente grafico, è necessario che l'interfaccia sia connotata da un design semplice ed intuitivo. I simboli dei partiti elettorali devono essere chiari, facilmente distinguibili e della grandezza adeguata affinché possano essere riconosciuti con un certo grado di facilità. Il design dell'interfaccia di voto, poi, è funzionale per l'espressione della preferenza da parte dell'elettorale, il quale deve essere posto nelle condizioni di poter scegliere il partito di predilezione in maniera semplice e immediata. Inoltre, l'elettore deve essere messo nella condizione di poter riflettere sulla scelta effettuata fino a che la procedura non si sia perfezionata. Ulteriore considerando in materia è il seguente. Se nella modalità tradizionale si dà per assodato che il voto sia valido e computato nel conteggio finale, a meno che l'elettore non abbia volutamente espresso un voto nullo, nella modalità digitale, invece, è necessario l'invio da parte del sistema di un avviso all'elettore circa l'inoltro del suo voto al server per il conteggio

[386] Gometz, 2017
[387] *Ibidem*

e il perfezionamento della procedura. È una sorta, se si può dire, di quietanza di ricezione di quanto avvenuto che assicura l'elettore sull'andamento a buon fine dell'iter.

Non vi sono dubbi, poi, sui vantaggi del *remote Internet voting* soprattutto per gli elettori. Il RIV garantirebbe una maggiore accessibilità consentendo anche a persone con disabilità o con difficoltà motorie di esercitare il diritto al voto senza la necessità di recarsi fisicamente alle urne. Inoltre, il poter votare liberamente in qualsiasi momento e da qualsiasi luogo, anche al di fuori del territorio nazionale, consente di ridurre costi in termini di tempo e di trasporto. Non si avrebbe la necessità, infatti, di prenotare aerei, treni o semplicemente di recarsi in auto alla propria circoscrizione per appore un "semplice" simbolo sul partito di preferenza. Inoltre, il RIV risulta essere compatibile con lo stile di vita contemporaneo che è dinamico, sempre in movimento ed è molto più frequente avere il cellullare sottomano o un computer che la tessera elettorale, la quale spesso e volentieri viene smarrita o non si ricorda più dove è stata riposta dopo le ultime consultazioni elettorali. Dal punto di vista democratico, il *remote Internet voting* sarebbe un valido aiuto nell'aumentare la partecipazione elettorale, soprattutto dei più giovani i quali hanno una certa dimestichezza con la tecnologia, vista l'assoluta libertà garantita con tale modalità di voto. Infine, il conteggio dei voti è più veloce in quanto effettuato da un apposito server, perciò vi è una drastica riduzione in termini di tempistiche e di errore umano che comporta conseguentemente una riduzione del contenzioso elettorale e il venir meno di una situazione di assoluta incertezza circa l'esito.

3.1.1. Il funzionamento del remote Internet voting

Venendo, poi, al funzionamento del *remote Internet voting* estone si osserva come esso sia costituito da una pluralità di elementi. Per quanto riguarda la procedura di identificazione dell'elettore vi è l'*Electronic Population Register,* un database nazionale che contiene i dati in formato digitale dei cittadini estoni e dei residenti stranieri dotati di permesso di soggiorno. Questo database è collegato a tutte le banche dati presenti su X-Road al fine di una connessione tra i server fornitori di diversi servizi pubblici[388]. Sempre in materia di identificazione, fin dal 1992 l'Estonia si è dotata di un sistema digitale di carta d'identità con il servizio di *e-identity* e di *ID-Card.* Questo sistema si fonda sul PIC, ossia il *personal identification number,* un codice univoco diverso per ogni cittadino e residente memorizzato nel chip della carta d'identità. L'*ID-Card* presenta due codici pin attraverso i quali è possibile accedere a tutti i servizi pubblici forniti dalla stessa, tra cui anche la votazione. Il primo codice pin consente di autenticare la propria identità al corrispondente servizio elettronico richiesto, mentre il secondo funge

[388] Sciannella, 2020

da firma elettronica sui documenti ai fini dell'approvazione delle transazioni online[389]. Il registro elettronico sulla popolazione e la carta d'identità elettronica sono gli elementi base del voto online, in quanto in loro assenza non è possibile esercitare tale diritto secondo questa modalità. L'*Electronic population register* è fondamentale, poiché secondo quanto previsto dal §5 del *Local Government Council Election Act* i cittadini estoni e i cittadini dell'UE che abbiano raggiunto di 18 anni di età al momento delle elezioni e coloro che risiedono in maniera permanente in Estonia hanno il diritto di votare. Pertanto, è necessario tenere un registro di coloro che possono esercitare tale diritto ai fini di una corretta identificazione. La carta d'identità elettronica, invece, è lo strumento che permette di accedere a tutti i servizi online forniti dall'*e-governance* estone rendendo, quindi, più accessibile l'esercizio del diritto al voto garantendo al contempo la presenza di sistemi di votazione multicanali per ridurre il problema del digital divide[390]. Nel concreto, la procedura di votazione tramite il *remote Internet voting* è piuttosto semplice. In primis, il sistema è dotato di due buste seguendo, quindi, l'*enevelope scheme* per cui vi è la busta interna, la quale contiene la scheda elettorale si presenta all'elettore una volta entrato all'interno del sistema con la scheda elettorale e la busta esterna, la quale contiene i dati identificativi dell'elettore. La piattaforma online viene attivata sette giorni prima dello svolgimento delle elezioni[391]. La ragione di tale attivazione anticipata rispetto all'*election day* consta nell'eliminare i doppi voti prima del conteggio ufficiale e di poter esercitare il diritto al voto nella modalità tradizionale qualora il sistema elettronico dovesse presentare dei malfunzionamenti, fungendo, per così dire, da backup. La procedura, poi, si articola nelle seguenti fasi. Il primo passo consiste nella corretta identificazione dell'elettore attraverso la *ID-Card* collegandosi da un computer dotato di *Vote Collector server*[392]. Una volta effettuato l'accesso, all'elettore si presenta la lista dei candidati. Il voto espresso viene, poi, firmato digitalmente dall'elettore in base ai requisiti dell'*Electronic Identification and Trust Services for Electronic Transactions Act*[393] ai sensi del §48[4] del *Riigikogu Election Act*[394]. Il voto così espresso, quindi viene inviato dal *Vote Collector server* ad un *Registration Service*. Questo service, poi, a seguito della corretta ricezione della preferenza espressa, elabora un *timestamp* che funge da quietanza di ricezione certificando il fatto che il voto è stato espresso e che la procedura è andata a buon fine[395]. Il *timestamp*, che si trova soprattutto

[389] *Ibidem*
[390] *Ibidem*
[391] *Ibidem*
[392] Ehin, Solvak, Willemson, & Vinkel, 2022
[393] È la legislazione nazionale che recepisce il regolamento n.910/2014 del Parlamento Europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno abrogante la direttiva 1999/93/CE. L'obiettivo di questo regolamento è di fornire una disciplina che provveda alla interoperabilità tra gli Stati membri in materia di identificazione elettronica. A tal fine, infatti, sono stati previsti standard procedurali e tecnici.
[394] https://www.riigiteataja.ee/en/eli/514122020002/consolide
[395] Ehin, Solvak, Willemson, & Vinkel, 2022

nell'ambito della blockchain, è essenziale perché dà la certezza all'elettore che la procedura è stata completata correttamente e che da quel momento in poi non è più possibile modificare la preferenza trasmessa. Infine, il voto correttamente trasmesso viene processato in un server adibito appositamente al ballottaggio per, infine, essere decriptato ed ottenere così il risultato[396]. Tale procedura, poi, può essere eseguita anche dal cellullare attraverso la scannerizzazione di un QR code e il modus operandi è lo stesso. Si osserva come la modalità sia alquanto semplice, poiché l'identificazione avviene attraverso la carta d'identità digitale, evitando conseguentemente possibili errori umani nella registrazione, per poi passare alla fase successiva che consiste nel mettere un click sul candidato preferito e inviare il voto. Il conteggio e l'elaborazione dei risultati non è affidato ad un essere umano, ma ad una serie di server e macchine in comunicazione tra di loro. Visto così, il *remote Internet voting* risulta essere allettante, tant'è che ci sono stati degli esperimenti in vari Paesi come la Norvegia nel 2011 e nel 2013 rispettivamente per elezioni locali e nazionali, come anche nel Regno Unito nel quinquennio 2002 – 2007 per le lezioni locali[397]. A tal proposito, infatti, ci si domanda come possa essere garantita la libertà e la segretezza del voto attraverso l'utilizzazione di tale sistema. Per quanto riguarda l'esperienza estone, si fa riferimento all'istituzione di commissioni nazionali pubbliche e private a presidio del corretto funzionamento della procedura e della sicurezza del sistema. Ad esempio, tra i numerosi organi costituiti si può fare riferimento alla *National Electoral Committee* disciplinata nel capitolo quattro del *Local Government Council Election Act* e nel capitolo quattro sottosezione uno del *Riigikogu Election Act.* Per quanto riguarda il primo testo di riferimento il §17 individua le competenze di tale commissione. In particolare, la *National Electoral Committee* ha il compito di garantire l'uniformità della condotta delle elezioni, istruire altre commissioni elettorali, esercitare la supervisione sulle proprie attività e su altre attività previste dalla legge[398]. Tra i poteri previsti, emerge in materia di votazione elettronica, la possibilità di non attivare la procedura, sospendere o concludere la votazione elettronica se si riscontrano problemi di sicurezza o di affidamento del sistema su cui poggia l'i-Voting tale per cui non è possibile garantirne il corretto funzionamento. Per quanto riguarda, invece, il secondo testo di riferimento, vengono disciplinati alcuni aspetti inerenti alla gestione delle elezioni. In particolare tale testo prevede il rispetto da parte della *National Electoral Committee* dei principi enunciati dal §1 dell'atto, il quale individua i principi del

[396] *Ibidem*
[397] Gli esperimenti di votazione elettronica al di fuori dell'Estonia non hanno avuto particolare successo principalmente per ragioni di sicurezza e per la mancanza di adeguate infrastrutture tecnologiche che consentissero un voto sicuro e trasparente. Si veda Sciannella, 2020.
[398] https://www.riigiteataja.ee/en/eli/514122020002/consolide

sistema elettorale[399] oltre all'assicurare una corretta procedura elettorale e supervisionare sull'attività degli *elections managers* ed esercitare ulteriori azioni che provengono dal sistema. Oltre alla presenza di commissioni nazionali, la segretezza del voto e la riservatezza della scheda elettorale sono garantiti dalla crittografia avanzata e da ulteriori tecnologie come la KSI blockchain, ossia *keyless signature infrastructure blockchain,* progettata e sviluppata in Estonia nel 2007 a seguito di un massiccio attacco hacker subito dall'infrastruttura digitale estone perpetrato dalla Russia causando il *Distributed Denial of Service*, uno degli attacchi informatici più comuni nel mondo hacker consistente nell'individuare siti web e server interrompendo i servizi di rete con l'obiettivo di esaurire le risorse di un'applicazione. In sostanza, in questa tipologia di attacco informatico vengono inviate enormi quantità di dati al sito web targetizzato causando rallentamenti fino ad arrivare ad un totale fuori servizio[400]. È curioso osservare come questi attacchi informatici siano stati distribuiti in tre periodi[401], ossia il 27 aprile 2007 giorno delle rivolte contro il Soldato di bronzo[402] raggiungendo il picco massimo al 3 di maggio e poi tra l'8 e il 9 maggio 2007 giorni simbolici di commemorazione della vittoria dei sovietici contro i nazisti. Si tratta, evidentemente, di commemorazioni ma anche di atti di "vendetta" nei confronti di uno dei Paesi dell'ex blocco che avrebbe voluto sortire l'effetto, probabilmente, di mettere a repentaglio l'intero apparato statale e mostrarne la debolezza. Al di là di questa guerra a livello informatico, tale evento è stato fondamentale per lo sviluppo di questa particolare forma di blockchain da parte dell'Estonia, più precisamente da Guardtime. Si tratta, in breve, di una blockchain che ha lo scopo di fornire un servizio di firma digitale. L'utente trasmette il valore di hash alla blockchain e in cambio riceve un token che prova la sua partecipazione alla rete blockchain[403]. Quest'ultima si basa sulla struttura ad albero, i cc.dd. *Hash Trees,* una delle prime forme di decentralizzazione conosciute nel mondo dell'informatica. La KSI non utilizza il sistema tradizionale di transazioni, ma i *timestamp* per creare e immagazzinare prove dell'esistenza dell'avvenuta operazione[404]. I *timestamp* si trasformano in *Hash Trees* e l'utente ottiene un token che prova l'avvenuta transazione. Si tratta di un sistema che sfrutta il meccanismo della blockchain rappresentandone, però, una variazione. Malgrado i numerosi vantaggi che tale sistema fornisce, è inevitabile sollevare qualche perplessità. Per cominciare, da alcuni esperimenti è risultato che le procedure di controllo sono inadeguate[405], in quanto non è stato seguito del tutto il protocollo o è stato seguito, ma in malo modo. Inoltre, si è osservato che

[399] Si fa riferimento ai seguenti principi: (i) il Riigikogu è composto da 101 membri, (ii) le elezioni sono libere, generali, uniformi e dirette; il voto è segreto, (iii) ogni elettore ha un voto e (iv) i risultati delle elezioni sono determinati in base al principio proporzionale. Tratto da https://www.riigiteataja.ee/en/eli/514122020002/consolide
[400] Tratto da https://www.microsoft.com/it-it/security/business/security-101/what-is-a-ddos-attack
[401] Tratto da https://www.theguardian.com/world/2007/may/17/topstories3.russia
[402] Monumento che ricorda i soldati sovietici caduti durante la seconda guerra mondiale.
[403] Matinovic, Kello, & Sluganovic, 2017
[404] *Ibidem*
[405] Springall, et al., novembre 2014

in presenza di un malfunzionamento del sistema, anziché andare a ricercare la radice del problema e risolverlo, il personale adibito a questa fase abbia semplicemente riavviato i server. È la logica del *se non funziona, spegni e riaccendi che funzionerà sicuramente*. Nello studio considerato[406], poi, gli autori hanno simulato un attacco informatico per testare la resilienza dell'infrastruttura digitale dal momento che viene decantata come una delle più sicure a seguito degli attacchi hacker del 2007. Il virus che è stato diffuso aveva intaccato la *ID-Card* verificando se fosse ancora inserita o meno all'interno del computer. Se era ancora presente all'interno del lettore, allora il virus creava una copia dell'i-Voting del client inviando un voto che andava a sostituire quello originariamente espresso. Ciò è alquanto grave, poiché l'elettore crede di aver votato per un determinato partito o candidato, quando la realtà dei fatti è diversa. Questo, quindi, comporta ad un possibile rischio di brogli elettorali. Nel caso in cui, invece, l'*ID-Card* dovesse essere stata rimossa, il virus rimane latente fino a che non viene inserita nuovamente. Si tratta di un attacco fantasma che è molto efficace, in quanto non vi sono particolari segni o avvertimenti ma se usato su larga scala potrebbe essere intercettato. Si presentano dunque problemi di natura tecnica. Oltre a queste criticità bisogna valutare come vengono garantiti i principi attinenti al voto, ossia la libertà, la segretezza e l'uguaglianza. In realtà, non si pongono molti problemi in materia, se non nel caso della segretezza. Come evidenziato in precedenza, il sistema del *remote Internet voting* estone appartiene alla forma di voto elettronico non presidiato, quindi il voto viene reso in assenza di un pubblico ufficiale. Questo valorizza la libertà, in quanto è possibile votare da qualsiasi device e in qualsiasi momento, ma non vi è la certezza di una totale assenza da coercizioni esterne che vadano a manipolare il volere dell'elettore. Per quanto concerne l'uguaglianza, invece, essa sarebbe comunque garantita in quanto il voto espresso attraverso la modalità online non ha un peso maggiore rispetto al voto espresso con la modalità tradizionale. Inoltre, qualora vi fosse un ripensamento, il voto online viene annullato una volta che l'elettore si reca alle urne ed esprime la sua preferenza sulla scheda compilativa. Ulteriore aspetto da considerare riguarda, poi, le elezioni. Esse devono essere generali, nel senso di accessibilità, per cui ogni cittadino deve essere posto nelle condizioni di poter votare. Non devono essere, quindi, presenti restrizioni di alcun tipo. Se si considera il voto online, però, emerge come l'essere dotati di una connessione alla rete Internet sia essenziale per poter esercitare comodamente e liberamente tale diritto e ciò comporta ad una potenziale restrizione dell'elettorato in quanto non è detto che tutti siano allacciati ad una rete Internet[407], soprattutto nelle zone più rurali. In conclusione si può affermare come l'Estonia sia riuscita a sfruttare a proprio favore una situazione di svantaggio iniziale diventando leader mondiale in materia di *e-governance* e di *e-*

[406] *Ibidem*
[407] Güven, 2020

democracy attraverso l'implementazione del *remote Internet voting*. Ciò che ha contribuito al successo di tale modalità è stata una costante educazione digitale della cittadinanza facendo sì che vi fosse un naturale passaggio dall'analogico al digitale. Si sono riscontrati alcuni incidenti di percorso, i quali si sono rivelati poi propizi per ulteriori sviluppi tecnologici e innovazioni in materia.

4. Italia: il Movimento 5 Stelle e la piattaforma Rousseau tra utopia e contraddizioni

Conclusa l'esposizione sull'esperienza estera dell'Estonia[408] e constatato che è l'unico Paese al mondo ad utilizzare il voto elettronico non presidiato per qualsiasi tipologia di elezione e come si sia giunti a questo importante risultato sfruttando una posizione di iniziale svantaggio seguita dalla ricostruzione del Paese a seguito della caduta della Cortina di ferro, si osserva come anche nel panorama italiano si ha avuto un assaggio di democrazia elettronica grazie al Movimento 5 Stelle[409] e all'utilizzo fino al 2021 della piattaforma di votazione elettronica fornita dall'Associazione Rousseau. Per comprendere l'importanza del partito in questione e come le numerose criticità siano state il fattore scatenante per porre un freno all'esperienza di *e-democracy*, bisogna considerare la storia del Movimento e del legame intercorrente con l'Associazione fondata da Casaleggio padre. La data ufficiale di fondazione del Movimento è il 4 ottobre 2009 che coincide con la celebrazione di San Francesco noto per essersi spogliato di tutti i beni. È una data simbolica che vuole fungere da messaggio agli avversari politici. Il messaggio è chiaro: noi del Movimento non siamo come voi classe dirigente che si preoccupa solo dei propri interessi, perché siamo vicino al popolo e diamo voce alle loro necessità. Il 4 ottobre 2009 è la data ufficiale, ma in realtà il Movimento 5 Stelle esisteva da ben prima con Beppe Grillo, noto comico genovese, e i suoi V-Day celebrati in varie piazze d'Italia, il più famoso è il V-Day di Bologna tenutosi a Piazza Maggiore, noto luogo di ritrovo della sinistra. Il Movimento, oltre a Beppe Grillo, aveva come volto noto Gianroberto Casaleggio, scomparso nel 2016, il quale ha avuto l'intuizione di creare una piattaforma online, Rousseau appunto, che consentisse agli iscritti al Movimento di esprimere elettronicamente le proprie preferenze circa le questioni poste dal partito. Non bisogna, dunque, confondere i due soggetti, ossia il Movimento 5 Stelle e l'Associazione Rousseau. Il M5S, infatti, è il partito politico, mentre l'Associazione Rousseau è il "fornitore" dei servizi di cui si è avvalso il Movimento. L'importanza del partito in questione e dell'utilizzo di Rousseau è assai evidente, in quanto segna una delle prime, se non la prima, esperienza di democrazia elettronica in Italia.

[408] Vi è un appunto da effettuare. Nonostante l'Estonia sia pioniera nel campo della votazione elettronica, bisogna osservare come la popolazione estone sia 1/3 della popolazione della provincia di Milano e con un'età media inferiore pari a 42 anni rispetto all'età media della popolazione milanese, la quale è di circa 45 anni. L'essere un popolo giovane e quantitativamente inferiore rispetto alla provincia di Milano, considerata a titolo di esempio, riduce notevolmente le problematiche di carattere tecnico e sociale consentendo, quindi, la sperimentazione in materia. Questi fattori, dunque, hanno contribuito al successo del *remote Internet voting* in Estonia.

[409] Da ora in poi abbreviato in M5S.

L'intuizione di Casaleggio padre, infatti, è geniale: il Movimento 5 Stelle è stato l'unico partito in tutta la storia della Repubblica a dotarsi di un servizio come Rousseau affinché le decisioni potessero essere prese non solo ai vertici, ma anche a livello degli elettori coinvolgendoli nei *lavori* del partito e consultandoli frequentemente su diverse tematiche. Vi è, quindi, una parvenza di democrazia diretta e di autogoverno del demos ristretto, però, agli iscritti al Movimento. Il partito, poi, è particolare perché fin dalle origini si è dichiarato antipartito, non avendo, per esempio, delle sedi fisiche in cui i vertici si riunissero né tantomeno una struttura organica ben organizzata. Il tutto cambia nel 2013, quando a seguito delle elezioni, il Movimento ottiene alcuni seggi alla Camera e al Senato per cui il partito si deve dotare necessariamente di una struttura più organizzata prevendendo, inoltre, un codice di condotta per i parlamentari. Osservando, poi, i valori promossi è interessante osservare come a seguito della sua entrata in Parlamento, il Movimento pur essendo tendenzialmente di sinistra, abbia strizzato l'occhio ad alcune politiche di destra e ad una parte del suo elettorato, nello specifico piccoli imprenditori e artigiani[410]. Non si può valutare quale sia stato l'esito di questa mossa, ma sicuramente essa ha giovato ad allargare la platea di potenziali iscritti al Movimento attratti dalla sua politica e dai valori promossi. Oltre a questo aspetto, il Movimento 5 Stelle è facilmente incasellabile all'interno della categoria dei partiti populisti, in quanto uno dei punti forti del suo programma è quello di essere anti – establishment, ossia l'essere contro la classe dirigente e quindi prevedere una serie di misure volte a ridurre o addirittura ad eliminare alcuni privilegi dell'establishment come tagli allo stipendio, limitazione del numero dei mandati rappresentativi e impedire ai parlamentari con condanne pendenti di essere eletti[411]. L'essere contro la classe dirigente al potere è uno dei tratti peculiari del populismo, oltre alla rievocazione della democrazia diretta andando conseguentemente ad instaurare un processo di disintermediazione attraverso l'utilizzo di piattaforme elettroniche che permettano agli iscritti di esprimersi su le più svariate tematiche. Alla fine il Movimento si tradisce nel suo intento di essere un partito antipartito, in quanto già a partire dal 2013 ha dovuto dotarsi di una struttura maggiormente organizzata e nel 2018, quando sale al Governo con la Lega, mostra ancora di più i suoi limiti dovendo effettuare un'opera di ristrutturazione interna, soprattutto a livello di leadership. Quando si parla dei pentastellati la prima persona che viene in mente è Beppe Grillo, ma ormai la sua figura non è più così rilevante all'interno del partito. Il volto del partito è rappresentato non tanto, quindi, dal fondatore ma dal leader politico del momento che guida il partito. Insomma, l'ascesa a Montecitorio ha fatto sì che si avverasse il passaggio da partito outsider a partito vero e proprio, tradendo, quindi, la propria identità.

[410] Tronconi, 2022
[411] *Ibidem*

4.1. La piattaforma Rousseau e i provvedimenti del Garante per la protezione dei dati personali

Spostando l'attenzione dal Movimento 5 Stelle all'Associazione Rousseau, fornitrice della piattaforma di votazione elettronica, emergono alcune problematicità che hanno posto un freno all'esperienza di *e-democracy* in Italia. In primis, per quanto riguarda la piattaforma Rousseau sono assenti dati, informazioni o documentazione che ne attestano o che ne spieghino l'operatività. In secondo luogo, dalle poche informazioni presenti risulta che la piattaforma Rousseau è stata sviluppata con un codice sorgente chiuso[412], il che vuol dire che solo l'azienda proprietaria può modificarlo e porre rimedio ad eventuali fallacie del software. Un programma, invece, generato con un codice sorgente aperto è pubblico e consente a chiunque di scaricare il codice, modificarlo e apporre migliorie. L'aver scelto un codice sorgente chiuso rappresenta una scelta strategica, in quanto eventuali problematiche legate soprattutto all'aspetto della sicurezza non verrebbero immediatamente in luce. Non si è a conoscenza, dunque, di eventuali falle del sistema né tantomeno se sono in corso operazioni di profilazione degli utenti. In terzo luogo, circa il funzionamento della piattaforma gestita dall'Associazione Rousseau è noto come essa sia stata più volte nel corso degli anni vittima di numerose incursioni e di attacchi informatici andando, quindi, a smentire la robustezza del codice sorgente chiuso del software. Ad esempio, nell'agosto del 2017 il sistema è stato hackerato da un *white hat*, ossia da un hacker etico le cui capacità informatiche vengono sfruttate dalle aziende per effettuate test sulla vulnerabilità del sistema, il quale scrive il seguente messaggio sulla pagina della piattaforma: *"Questa pagina non è un attacco politico. È stata pubblicata solo con l'intento di rendere trasparente e semplice una questione importante. I dati personali di molte persone erano ottenibili a causa di una vulnerabilità presente nel sito"*[413]. Qualche giorno dopo, l'account Twitter Rouge0 pubblica le liste dei nomi, mail, cellulari di alcuni ministri pentastellati. Queste incursioni rendono alquanto evidente come la piattaforma non sia resiliente alle aggressioni informatiche e mette in risalto alcune criticità che sono state successivamente riprese anche dal Garante per la protezione dei dati personali[414] a seguito delle segnalazioni che traggono origine da questi eventi. In particolare, faccio riferimento al provvedimento n.548 del 21 dicembre 2017 in materia di data breach e il successivo provvedimento n.83 del 4 aprile 2019. Per quanto riguarda il provvedimento del 2017, viene analizzato il data breach dell'agosto dello stesso anno da parte dell'utente Twitter Rouge0. Egli, oltre ad essere entrato nel sistema della piattaforma Rousseau pubblicando indirizzi mail e numeri cellulari, ha anche inserito alcuni post sul sito www.movimento5stelle.it impersonando altri utenti e ha effettuato un login sul blog

[412] *Ibidem*
[413] *Ibidem*
[414] Da ora in poi abbreviato in GPDP

www.beppegrillo.it utilizzando le credenziali degli utenti registrati. Emerge, dunque, che non è solo il sito della piattaforma Rousseau ad essere sottoposto ad un attacco informatico, ma anche gli altri due siti afferenti al partito. L'intero apparato risulta essere vulnerabile dando vita ad un paradosso. Il Movimento 5 Stelle si propone come esempio di democrazia elettronica utilizzando le ICT nei processi decisionali all'interno del partito per favorire il coinvolgimento degli iscritti, ma allo stesso tempo non si è dotato degli strumenti informatici adeguati a raggiungere tale scopo. A seguito delle segnalazioni effettuate al Garante, esso ha effettuato una serie di verifiche su più fronti. In primis, l'Autorità è andata a controllare lo svolgimento delle procedure di autenticazione online osservando come per la registrazione sul sito del Movimento e sul sito di Rousseau[415] vi sia un modulo di iscrizione comune afferenti a due tipologie di registrazione. La prima è quella base che consente solo l'accesso al sito del Movimento, mentre la seconda, ossia la registrazione verificata attraverso il caricamento della carta d'identità consente di sfruttare tutte le funzioni della piattaforma Rousseau. Il Garante ha rilevato come la procedura di registrazione sia alquanto debole, dal momento che la password scelta dall'utente poteva essere inferiore agli otto caratteri e quindi particolarmente semplice da decriptare[416]. È lapalissiano, dunque, come i dati personali degli utenti non siano al sicuro e come essi possano essere facilmente diffusi. A tal proposito il Garante, infatti, ritiene che sia essenziale individuare chi sia il titolare del trattamento dei dati personali e il responsabile del trattamento dei dati personali, in quanto sono due soggetti distinti. All'articolo 4 del GDPR[417] per titolare del trattamento si intende un soggetto che determina le finalità e i mezzi di trattamento dei dati personali, mentre per responsabile del trattamento si intende un soggetto che tratta i dati per conto del titolare. Egli, dunque, effettua le operazioni afferenti all'utilizzazione ed elaborazione dei dati seguendo le indicazioni del titolare del trattamento. Il Garante non individua chi siano tali soggetti, ma si può affermare con un certo grado di certezza come il titolare del trattamento sia il Movimento 5 Stelle, mentre il responsabile del trattamento sia la piattaforma Rousseau, la quale detiene i dati personali degli iscritti e ne dispone. Ciò che emerge dall'analisi del Garante è che tra i soggetti titolari del trattamento dovevano essere compresi anche WindTre SPA e ITNET SRL, ergo si riscontra una illiceità del trattamento poiché vi è stata una comunicazione riguardante i dati personali a soggetti terzi in mancanza del consenso degli interessati[418]. Ulteriore rilievo riguarda la sicurezza informatica della piattaforma Rousseau, il punto cruciale dell'intera vicenda. È stato osservato come il *content managment system,* ossia il CMS, sia obsoleto sia per il portale web del Movimento sia per il blog di Beppe Grillo. L'obsolescenza riguarda

[415] www.rousseau.movimento5stelle.it
[416] Garante della protezione dei dati personali, 2017
[417] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio.
[418] Garante della protezione dei dati personali, 2017

il rischio di una possibile fuga di dati, in quanto essendo versioni risalenti e non aggiornate, si corre il pericolo di accessi abusivi al sistema. Nello specifico, in base all'articolo 25 del GPDR è previsto il principio del *data protection by design*, ossia il titolare del trattamento assicura il corretto trattamento dei dati personali attraverso le più adeguate misure tecniche e organizzative. Per garantire il rispetto del principio del *data protection by design,* si fa riferimento (i) alla quantità di dati raccolti, (ii) alla portata del trattamento, (iii) al periodo di conservazione e (iv) all'accessibilità[419]. Il *data protection by design*, inoltre prevede che le misure adottate dal titolare del trattamento garantiscono che "*non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica"*[420]. L'ultimo profilo da esaminare riguarda l'opinione del Garante in tema di voto elettronico con riferimento al profilo della riservatezza. Il problema rilevato dall'Autorità riguarda l'associazione della preferenza espressa elettronicamente al numero telefonico dell'individuo che ha proceduto alla votazione. Non viene garantita, dunque, la riservatezza del voto in quanto è agevole risalire dal numero di cellullare al nome e cognome del votante consultando il database anagrafico della piattaforma. Non vi è, una volta conclusa la procedura di votazione, una procedura adibita alla pseudonimizzazione o anonimizzazione, oltre alla previsione di un termine decorso il quale le informazioni riguardanti i votanti vengano rimosse o anonimizzate. Viene, di conseguenza, violato il principio della *data protection by design* come previsto dall'art.25 del GDPR. A seguito delle criticità rilevate, il Garante per la protezione dei dati personali ha prescritto una serie di misure da adottare per evitare futuri data leak. Tra queste, si fa riferimento (i) all'adozione di adeguate azioni di *vulnerability assesment*, ossia una valutazione della vulnerabilità del sistema, per correggere eventuali debolezze nei servizi prima della fruizione al pubblico, (ii) all'adozione di un sistema di identificazione informatica degli utenti tale per cui le password siano sicure in base ad una serie di parametri, tra cui l'essere minimo di otto caratteri, (iii) conservare le password utilizzando un sistema di algoritmi crittografici e (iv) l'adozione di protocolli HTTPS per i siti web.

Successivo al provvedimento del 2017, vi è il provvedimento del 4 aprile 2019 n.83. Lo scopo è verificare se le misure prescritte nel provvedimento del 2017 siano state rispettate o meno. Si constata come ci sia stata una ristrutturazione del sito www.beppegrillo.it con conseguente trasferimento su una nuova infrastruttura informatica, la quale non consente più la creazione di account personali[421]. Per quanto riguarda l'Associazione Rousseau vi è stato l'espletamento di tutti gli adempimenti previsti. Il Garante, dunque, ha proceduto ad un'indagine ispettiva per verificare la robustezza dei sistemi di sicurezza adottati rispetto alle criticità emerse. Da questa indagine, spiccano i seguenti risultati. In

[419] Art.25 co.2 GDPR
[420] Art.25 co.2 GDPR
[421] Garante per la protezione dei dati personali, 2019

punto di *vulnerability assesment*, l'Associazione Rousseau afferma che i punti più deboli del sistema sono stati affrontati e il Garante dà atto di ciò. In riferimento, invece, all'utilizzo di algoritmi crittografici deboli e all'obsolescenza tecnologica del CMS soprattutto per lo storaggio delle password è stato rilevato come si siano abbandonati i sistemi obsoleti per adottare, invece, algoritmi crittografici robusti. Un ulteriore rilievo, poi, riguarda l'adozione di protocolli di rete sicuri per evitare le trappole in Rete, ossia siti web che hanno una dicitura simile ai siti originali ma che si differenziano per una lettera in più o in meno o per il mancato utilizzo di un protocollo di rete sicuro. Constatato questo, la valutazione del Garante è parzialmente positiva, in quanto nonostante i soggetti coinvolti abbiano cercato di seguire le prescrizioni previste dall'Autorità rimangono ancora dei nervi scoperti. Per esempio, in materia di valutazione della vulnerabilità dei sistemi, malgrado ci sia stato un miglioramento a livello della sicurezza, permangono delle criticità circa l'obsolescenza di alcuni componenti del software dei siti web del Movimento.[422] In punto di riservatezza delle operazioni di voto elettronico si è osservato che per garantire tale principio non è sufficiente l'aver rimosso il numero di telefono associato al votante, in quanto sono presenti ulteriori elementi identificativi univoci dell'iscritto che permettono facilmente di associare il voto espresso alla persona dell'iscritto[423]. Infine, il provvedimento del 2017 aveva rilevato come vi fosse la condivisione di un unico modulo di iscrizione sia per il sito www.movimento5stelle.it e per il sito www.rousseau.movimento5stelle.it. Il Garante nel provvedimento del 2019 rileva come l'utilizzo delle stesse credenziali che consente di accedere a più sistemi ponga dei problemi in materia di sicurezza, problemi che non erano stati ancora affrontati né dal Movimento né dall'Associazione Rousseau. L'Autorità, dunque, ordina ai soggetti coinvolti di rimuovere le criticità emerse a seguito dell'accertamento ispettivo. Inoltre, è stato ordinato di provvedere ad assegnare credenziali di autenticazione ad uso esclusivo di ciascun utente e non consentire più, quindi, l'utilizzo delle stesse credenziali per accedere ad una pluralità di sistemi ed informazioni. L'Autorità, poi, ha stabilito un periodo di 120 giorni dalla ricezione del provvedimento per controllare nuovamente se vi è stata l'adozione delle misure di sicurezza prescritte e a 60 giorni dalla ricezione del provvedimento, invece, è stata prevista una valutazione circa la protezione dei dati, soprattutto in riferimento alle funzionalità di votazione elettronica, in quanto è stato rilevato come l'aver dissociato il numero di telefono dell'utente al voto espresso non è una misura sufficiente per garantire la protezione dei dati[424]. Traendo le fila, dunque, si può affermare come la valutazione del Garante sia stata parzialmente positiva, in quanto l'Autorità ha riscontrato ancora delle problematiche

[422] *Ibidem*
[423] *Ibidem*
[424] *Ibidem*

rispetto al provvedimento del 2017 tali per cui si è reso necessario un suo ulteriore intervento in materia.

L'Associazione Rousseau non si occupava solo di gestire la piattaforma di votazione elettronica del Movimento, ma anche una serie di applicazioni e/o funzioni ulteriori che andrebbero ad arricchire il concetto di democrazia elettronica. In particolare, la funzionalità lex iscritti desta qualche curiosità. Tale funzione, infatti consente ad ogni iscritto al Movimento di presentare una proposta di legge, la quale dopo un lungo iter di approvazione giunge in Parlamento per essere tradotta, eventualmente, in un disegno di legge[425]. Tutto ciò è pura utopia, in quanto l'uomo comune non è dotato delle competenze necessarie per la redazione di un testo che corrisponda agli interessi della collettività e che sia dotato delle caratteristiche della generalità e dell'astrattezza. Si corre il rischio, poi, di presentare in Parlamento delle leggi *ad personam,* che non rifletterebbero, invece, i bisogni della comunità tutta ma di un ristretto gruppo di persone. Ad esempio, attraverso questa piattaforma sarebbe possibile redigere una proposta di legge che preveda l'esenzione dalla tassazione di alcune categorie di commercianti andando, invece, a danneggiarne altri. Si tratta, quindi, di uno strumento che in apparenza conferisce un certo grado di potere all'uomo comune di farsi Legislatore, ma allo stesso tempo non assicura la qualità delle proposte in essere. Gli iscritti all'Associazione, inoltre, venivano e vengono consultati frequentemente. Nello Statuto attuale, come anche quello precedente, non sono molte le regole di carattere procedurale che indicano lo svolgimento delle consultazioni online, l'unica prescrizione si trova all'art.7 lettere d), e), f), g) e h). Lo Statuto attuale non indica quanto prima deve essere effettuata la convocazione, ma ne indica il contenuto, ossia (i) l'argomento o gli argomenti oggetto della votazione, (ii) la data e l'orario iniziale e finale, (iii) la modalità di voto e (iv) la durata della consultazione che non può essere inferiore a dieci ore. Inoltre non possono votare gli iscritti da meno di sei mesi, coloro che sono stati sospesi, coloro che sono stati esclusi dall'Associazione e i sostenitori. Altra peculiarità è che non vi è un quorum minimo, per cui le decisioni rimesse agli iscritti del M5S sono approvate *"qualunque sia il numero di partecipanti al voto"*[426]. Questo è un dato assai rilevante, poiché le decisioni vengono assunte indipendentemente dall'affluenza, il che è alquanto rischioso poiché si corre il pericolo dell'instaurarsi di una democrazia della minoranza. In tal senso, dunque, pochi soggetti prendono decisioni su tematiche assai rilevanti che coinvolgono l'intera collettività traendo beneficio dall'astensionismo. Il caso più clamoroso che funge da esempio su come funzionasse la piattaforma Rousseau e di come in realtà ciò che è promosso dal Movimento è un'apparente *e-*

[425] (Villaschi, 2020)
[426] Art.7 lett. d) dello Statuto del M5S del 2021

democracy è la votazione sul cc.dd. Caso Diciotti[427]. All'epoca era vigente il vecchio Statuto, il quale prevedeva ventiquattrore di preavviso prima della consultazione vera e propria. È stata una delle consultazioni con il maggior numero di votanti in una sola giornata che ha avuto come risultato la negazione dell'autorizzazione a procedere. Il quesito, in particolare, era stato formulato nei seguenti termini: "*Il ritardo dello sbarco della nave Diciotti, per redistribuire i migranti nei vari paesi europei, è avvenuto per la tutela di un interesse dello Stato? – Sì, è avvenuto per la tutela di un interesse dello Stato, quindi deve essere negata l'autorizzazione a procedere; - No, non è avvenuto per la tutela dell'interesse dello Stato, quindi deve essere approvata l'autorizzazione a procedere"*[428]. Il risultato è scontato considerato che all'epoca il Movimento era al Governo assieme alla Lega, poiché se avesse vinto l'autorizzazione a procedere ciò sarebbe stato il fattore scatenante per una crisi di Governo e conseguenti elezioni anticipate. Al di là di questo aspetto, ciò che emerge è la mancanza di dialogo, poiché si tratta di un quesito posto in forma referendaria con un sì o un no senza dare spazio al dibattito. Il dibattito, inoltre, non poteva essere intavolato in quanto vi era stato uno scarso preavviso per la votazione imminente e di conseguenza è stato un voto espresso, per così dire, a sentimento anziché essere il frutto di una lunga e attenta riflessione. È chiaro, dunque, come il Movimento 5 Stelle pur essendo stato innovativo nella scena politica italiana, in realtà ha mostrato i limiti della democrazia elettronica, almeno in Italia. Queste forme di consultazione online non son idonee ad ottenere una risposta immediata a tematiche complesse, le quali, invece, richiedono un confronto che sia il più costruttivo possibile per giungere ad un risultato che sia soddisfacente per la maggior parte.

4.2. La separazione da Rousseau e il passaggio a Skyvote

Alla luce delle dinamiche sopra esposte, si può affermare che l'intuizione di Casaleggio padre era sì geniale, ma i tempi erano prematuri per mettere in azione il suo piano. A seguito del divorzio da Rousseau, avvenuto nel 2021 per ragioni economiche[429], ad oggi il Movimento 5 Stelle utilizza un nuovo sistema di votazione elettronica fornito dalla piattaforma Skyvote di proprietà della società Multi cast che opera dal 2014 nel settore del voto elettronico. Skyvote tra i vari servizi offerti, prevede anche Skyvote election, ossia una soluzione per il voto elettronico sia online che in presenza. La scelta

[427] Matteo Salvini, ex Ministro dell'interno, era stato accusato di sequestro di persona aggravato. Il 16 agosto 2018 la nave Ubaldo Diciotti della guardia costiera italiana ha soccorso 190 persone in acque internazionali vicino a Malta. Le autorità italiane sapevano della loro presenza già dal 14 agosto. Il 20 agosto – quando la nave approda a Catania – il comandante riceve l'ordine di non calare la passerella per far scendere i migranti. L'ordine proviene dal Ministero dell'Interno. I migranti sono stati autorizzati a scendere solo al 26 di agosto. Tratto da https://www.internazionale.it/bloc-notes/annalisa-camilli/2019/02/18/diciotti-matteo-salvini

[428] Villaschi, 2020

[429] Il Movimento era in debito nei confronti dell'Associazione Rousseau per una cifra corrispondente a più di € 400.000. Il Movimento, infatti, versava periodicamente delle somme di denaro all'Associazione per i servizi resi.

di tale piattaforma è scaturita, molto probabilmente, dalle lezioni apprese con la piattaforma gestita dall'Associazione Rousseau e dai numerosi problemi in materia di sicurezza. In primis, come dichiarato dallo sviluppatore di Skyvote, il rapporto intercorrente tra il Movimento e il nuovo provider di servizi è puramente professionale, senza alcun coinvolgimento politico come, invece, era successo in passato[430]. Skyvote, inoltre, non raccoglie i dati degli utenti registrati al servizio, ma li utilizza temporaneamente per l'identificazione dell'elettore al momento del collegamento al sistema di voto, altra grande differenza rispetto a Rousseau. Per quanto riguarda la procedura di votazione è necessario essere collegati ad una rete Internet su un dispositivo fisso o mobile e utilizzare un Internet browser compatibile con il programma, tra cui Safari, Google Chrome, Mozilla Firefox e Microsoft Edge. Nei giorni antecedenti alla votazione, gli elettori ricevono una comunicazione con un link di accesso alla cabina virtuale. Una volta cliccato, si accede alla cabina di votazione e si procede alla identificazione. Conclusa la procedura di identificazione, si presenta la scheda di voto ed esprimere la propria preferenza. Successivamente viene inviato un codice OTP, ossia one time password, al numero di cellulare indicato da inserire nell'apposito spazio per confermare definitivamente il voto. Se la procedura va a buon fine, compare la ricevuta di voto con un codice univoco che accerta la corretta acquisizione del voto[431]. Come si evince dalla procedura appena descritta, essa è semplice ed intuitiva. Il Movimento non ha rinunciato ad un elemento essenziale della sua identità, ossia l'affidarsi a soggetti terzi per la fornitura e gestione della votazione elettronica cercando di mettere in atto la *e-democracy.* In conclusione si può affermare come il Movimento 5 Stelle abbia tra le numerose difficoltà di percorso cercato di porsi come propulsore della democrazia elettronica in Italia mostrandone i limiti e le contraddizioni. Difatti, da partito antipartito ha tradito parte della sua identità dovendosi trasformare, a seguito dell'ascesa a Montecitorio, in un partito vero e proprio. Vi sono state numerose criticità con la piattaforma Rousseau e i rapporti con l'Associazione con il passare del tempo sono diventati sempre più tesi fino a che nel 2021 non vi è stata la rottura definitiva per una mera questione economica. Questo fa riflettere, in quanto viste le criticità emerse in riferimento al funzionamento della piattaforma ci si sarebbe aspettati un abbandono da parte del Movimento, invece si è verificato il contrario. È stata, forse, una mossa poco elegante quella dell'Associazione Rousseau dal momento che era l'unico fornitore per tutti i servizi, dalla comunicazione alla votazione, del partito. Nel male, però, il Movimento ha appreso la lezione, difatti nel nuovo Statuto all'articolo 1 lett. e) è previsto che per tutte le attività di consultazione dei propri Iscritti *"si potrà ricorrere a piattaforme digitali e/o strumenti informatici propri o affidati a società di servizio anche esterne. Queste prestazioni saranno regolate*

[430]https://www.repubblica.it/tecnologia/2021/06/15/news/skyvote_al_posto_di_rousseau_m5s_rassicura_i_dati_sono_al_sicuro-306162854/
[431] https://www.movimento5stelle.eu/votazione/

da specifici accordi […]"[432]. Nel testo non vi è alcuna specificazione riguardo alle piattaforme utilizzate né tanto meno alcuna clausola che prevede un vincolo di unicità per cui vi è un solo fornitore per tutti i servizi. In conclusione, se in Estonia si è stati in grado di sfruttare il carpe diem per dare vita ad un sistema di votazione elettronica in auge da quasi vent'anni, in Italia i tempi erano ancora troppo acerbi per poter implementare la democrazia elettronica. Il tentativo, però, è stato encomiabile in quanto ha aperto le porte ad una riflessione sulle potenzialità, contraddizioni e problematicità della democrazia elettronica su più fronti da quello giuridico a quello tecnico a quello sociale. Nel prossimo capitolo si studierà il voto elettronico e la tecnologia applicata al settore elettorale presentando le più celebri piattaforme di voto elettronico, le opportunità offerte da questa tecnologia e i suoi aspetti oscuri.

[432] Movimento 5 Stelle, 2021

CAPITOLO IV: BLOCKCHAIN E VOTO ELETTRONICO.

1. La nozione di voto elettronico

Nel precedente capitolo si è esaminato il tema della democrazia elettronica mettendone in luce i vantaggi nonché gli aspetti più critici. Si è discusso, poi, delle ragioni che hanno portato alla teorizzazione di tale concetto individuate nella perdurante crisi della democrazia rappresentativa, nonché nell'ingerenza dei nuovi canali di comunicazione in politica che ha comportato ad un profondo mutamento nel rapporto tra elettorato e corpo politico. Per quanto attiene all'aspetto della crisi della democrazia rappresentativa si è sottolineato il crescente astensionismo tra gli elettori che non dipende solamente da una forma di *protesta,* ma anche da oggettive impossibilità a prendere parte al suffragio determinate principalmente da problemi di salute e dall'essere residenti in un territorio che è al di fuori della propria circoscrizione elettorale. Una delle soluzioni per contrastare l'astensionismo e favorire una maggior partecipazione elettorale è il voto elettronico. A tal proposito, spesso il concetto di *e-democracy,* ossia "*l'uso delle ICT come mezzo per lo svolgimento delle procedure di autogoverno del demos*"[433] viene confuso con il voto elettronico, in quanto i confini tra i due termini non sono molto chiari. L'origine di questa sovrapposizione consiste nel fatto che la democrazia elettronica viene vista come una delle tante forme attraverso le quali i cittadini partecipano alla formazione delle decisioni che riguardano la collettività[434]. Anche l'esercizio del diritto al voto è una forma di partecipazione dei cittadini alla formazione di decisioni che coinvolgono la collettività, in quanto vengono chiamati ad eleggere i loro rappresentanti in Parlamento. Il rapporto, dunque, tra democrazia elettronica e voto elettronico non è di carattere *interscambiabile,* inteso nel senso che l'utilizzo di una espressione al posto dell'altra afferisce allo stesso concetto, ma si tratta di un rapporto *genus* a *species.* Il *genus* è rappresentato dalla democrazia elettronica, la quale è una particolare forma di governo teorizzata come possibile alternativa alla democrazia rappresentativa. La *species,* invece, è il voto elettronico, il quale rappresenta uno strumento differente rispetto alla modalità di votazione tradizionale attraverso il quale si svolgono i procedimenti democratici. Chiarito, quindi, questo aspetto il presente paragrafo cercherà di fornire una panoramica per quanto più esaustiva possibile sulla nozione di voto elettronico. La ricerca di modalità alternative di espressione del suffragio è un tema ricorrente nell'ambito politico – giuridico tant'è che si ripresenta ciclicamente all'esito di ogni elezione, o quasi, essendo preoccupante

[433] Gometz, 2017
[434] *Ibidem*

il tasso di astensionismo tra gli elettori[435]. Nel panorama europeo a partire dai primissimi anni 2000 il Consiglio d'Europa ha fornito una prima definizione di voto elettronico nel senso di *"an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote"*[436]. Il tenore della definizione è ampio, poiché all'interno di essa si fa riferimento sia alle consultazioni elettorali sia a quelle referendarie le quali prevedono in entrambi i casi il coinvolgimento di strumenti tecnologici quantomeno nella fase dell'espressione del voto. Nel preambolo della Raccomandazione del 2004 si prende atto di come le ICT siano sempre più presenti nella vita quotidiana invitando, dunque, gli Stati membri a monitorare l'evoluzione di tali tecnologie e la loro possibile implementazione nei processi democratici[437]. Sono i primi passi che portano ad una riflessione su tale tema, riflessione che si rinnova nella successiva Raccomandazione del 2017 nella quale il Consiglio d'Europa definisce il voto elettronico come l'utilizzo di strumenti elettronici per l'espressione e/o il conteggio del voto[438]. La definizione del 2017 apparentemente non è cambiata, ma la dicitura del 2004 e in particolare "*at least in the casting of the vote"* è l'elemento chiave che consente di affermare come la nozione del 2017 sia diversa, in quanto nel voto elettronico viene considerato non solo l'espressione della preferenza, ma anche il conteggio del voto stesso. Il testo originale del 2017, infatti, descrive l'*e-voting* come "*the use of electronic means to cast and/or count the vote".* Per quanto riguarda, invece, il panorama italiano a partire dal 2020 vi è stato l'avvio di un iter per la sperimentazione e la possibile utilizzazione del voto elettronico alle elezioni politiche ed europee e per i referendum abrogativo disciplinato dall' art.75 della Costituzione e costituzionale ex art.138. In particolare, nella legge di bilancio n.160/2019 all'art.1 i commi 627[439] e 628[440] hanno previsto lo stanziamento di un fondo per il voto elettronico pari a un milione di euro per l'anno 2020, rinnovato dall'art.6 co.3 del d.l.n.41/2022[441], e un decreto del Ministro

[435] A titolo di esempio si considerando le ultime elezioni politiche nazionali del 2022, in cui il tasso di astensione ha raggiunto il 36,27% rispetto alle elezioni del 2018 in cui il tasso di astensionismo era parti al 27,1%. Vi è stato un incremento di circa nove punti percentuali degli elettori che si sono astenuti. Tratto da https://www.econopoly.ilsole24ore.com/2022/11/04/elezioni-voto-cambiamento/

[436] Council of Europe, 2004

[437] Il testo originale prevede: *"Recognising that as new information and communication technologies are increasingly being used in day – to – day life, member states need to take account of these developments in their democratic practice".*

[438] Council of Europe, 2017

[439] Art.1 co.627 l.n.160/2019: *"Allo scopo di introdurre in via sperimentale modalità di espressione del voto in via digitale per le elezioni politiche ed europee e per i referendum previsti dagli articoli 75 e 138 della Costituzione, è istituito nello stato di previsione del Ministero dell'Interno il Fondo per il voto elettronico con uno stanziamento di un milione di euro per l'anno 2020".*

[440] Art.1 co.628 l.n.160/2019: *"Con il decreto del Ministro dell'Interno, di concerto con il Ministro per l'innovazione tecnologica e la digitalizzazione, da attuare entro trenta giorni dalla entrata in vigore della presente legge, sono definite le modalità attuative di utilizzo del Fondo di cui al comma 627 e della relativa sperimentazione limitata a modelli che garantiscano il concreto esercizio del diritto di voto degli italiano 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".*

[441] Art.6 co.3 d.l. n.41/2022: *"In considerazione della situazione politica internazionale e correlati rischi connessi alla cybersicurezza, l'articolo 1, comma 628, secondo periodo della legge 27 dicembre 2019, n.160, si applica per l'anno 2023.*

dell'Interno definenti le modalità attuative di utilizzo dei fondi messi a disposizione. A seguito delle disposizioni citate, con il decreto ministeriale del 9 luglio 2021 sono state individuate le linee guida per la sperimentazione della modalità di espressione del voto in via digitale. Non si tratta, però, di una sperimentazione aperta a tutti i cittadini, in quanto si rivolge solamente ad un pubblico ristretto, ossia a coloro che risiedono all'estero o che per una serie di motivi[442] risiedono in un Comune di una Regione diversa da quella del Comune nelle cui liste elettorali risultano iscritti. È una sperimentazione, poi, circoscritta a determinati ambiti territoriali individuati sulla base di alcuni criteri quali, ad esempio, le infrastrutture presenti. Si può affermare come il legislatore abbia voluto fare piccoli passi verso il voto elettronico coinvolgendo i soggetti e i territori che ne trarrebbero maggior vantaggio. Inoltre, un'altra ragione per la quale la sperimentazione è così limitata è dovuta anche per questioni di budget considerato che i fondi stanziati ammontano in totale a due milioni di euro[443]. Sembra una cifra importante, ma se confrontata con i fondi messi a disposizione nella legge di bilancio del 2020 per altre opere come la messa in sicurezza di scuole, edifici pubblici e patrimonio comunale, che ammontano a quattrocento milioni di euro[444], i fondi previsti per la sperimentazione del voto elettronico risultano essere del tutto irrisori. Al di là di questo aspetto meramente economico, si può dare una prima definizione di voto elettronico nel senso di una modalità alternativa di espressione del suffragio consistente nell'ausilio supporti informatici. Su questo punto, difatti, è possibile tracciare una evoluzione circa la tecnologia utilizzata nei sistemi di votazione elettronica. I primi sistemi utilizzavano il metodo della scheda perforata, ossia il cc.dd. *punch card voting system.* Esso trae origine nell'invenzione Herman Hollerith a fine del XIX secolo. L'ingegnere statunitense inventò un macchinario utilizzato per la raccolta e l'elaborazione dei dati consistente nell'impiego di schede perforate e di un macchinario elettromeccanico nel quale grazie ai contatti elettrici con i fili metallici e attraverso i fori sulla scheda si era in grado di registrare il dato rilevato[445]. Tale sistema è stato utilizzato anche in ambito elettorale negli Stati Uniti fino al 2000, anno dal quale è stata dismessa tale modalità di votazione[446]. L'evoluzione dell'espressione del suffragio attraverso la scheda perforata è

A tal fine il Fondo per il voto elettronico istituito nello stato di previsione del Ministero dell'interno dall'art.1, comma 627, della legge 27 dicembre 2019, n.160, rifinanziato per 1 milione di euro per l'anno 2023".

[442] Le linee guida fanno riferimento a motivi di lavoro, studio e cure mediche. Si tratta di una elencazione di carattere tassativo delle ragioni per cui un cittadino si possa momentaneamente trovare in una Regione diversa rispetto alla quale risulta essere iscritto alle liste elettorali, nonché si tratta delle tre ragioni principali che inducono alla riflessione sul voto elettronico nelle democrazie odierne.

[443] Tenuto conto anche del rinnovo dello stanziamento dei fondi previsto dal d.l. n.41/2022

[444] Si veda la legge n.160/2019 art.1 commi 107 – 114

[445] Enciclopedia Treccani, voce Herman Hollerith

[446] Il problema attinente al punch card voting system riguarda il conteggio dei voti, poiché alcune schede elettorali non erano state perforate correttamente e il cc.dd. *chad,* ossia il pezzettino di carta che dovrebbe staccarsi all'esito della punzonatura, non era completamente staccato dalla scheda elettorale causando un problema nel conteggio dei voti, in quanto poteva trarre in inganno il macchinario utilizzato per il conteggio costringendolo a rifiutare la scheda elettorale e ritenere, quindi, che il voto non fosse stato espresso correttamente. Alle elezioni presidenziali del 2000 si verificò tale

rappresentato dall'*optical scanning voting system.* Secondo questo sistema, la scheda elettorale perforata dopo essere stata compilata viene inserita in un apposito macchinario, il quale procede alla sua lettura attraverso uno scanner ottico registrando così il segno apposto dall'elettore e il voto espresso[447]. Con il passare del tempo la scheda perforata venne abbandonata in favore del DRE, ossia del *Direct Electronic voting system,* il quale è ciò che nell'immaginario collettivo si avvicina maggiormente al voto elettronico. Nel DRE, infatti, vi è l'utilizzo di un macchinario a ciò specificatamente adibito attraverso il quale l'elettore esprime la propria preferenza alle urne scegliendo il candidato e/o il partito attraverso un *tap* sul touch screen o spingendo appositi pulsanti[448]. Le informazioni così ottenute, alla chiusura delle urne, vengono registrate e inviate ad un dispositivo di archiviazione esterna rimovibile come, ad esempio, una chiavetta USB. A tal proposito, per esempio gli Stati Uniti a seguito dell'abbondono del *punch card* passarono all'utilizzo nelle tornate elettorali del *Direct Recording Electronic voting system* e fu alquanto celebre e discusso il caso di DIEBOLD, il software utilizzato nei macchinari adibiti alla votazione elettronica[449]. Infine, vi è l'*Internet Voting system* conosciuto anche come *I-voting*, il quale rappresenta una particolare fattispecie di votazione elettronica, in quanto consente all'elettore di esprimere la propria preferenza grazie all'ausilio di una rete Internet permettendo, dunque, di esercitare il diritto al voto anche in contesti che si collocano al di fuori di quelli tradizionali, ossia le urne[450]. Ulteriore aspetto da considerare nel voto elettronico è la *forma* attraverso la quale la preferenza viene espressa o, meglio, sulla presenza o assenza di pubblici ufficiali attestanti la regolarità di tutte le procedure di votazione. Si fa riferimento al voto elettronico presidiato e al voto elettronico non presidiato. Per quanto riguarda il voto elettronico in forma

problematica nello Stato della Florida, il quale riportò che Bush aveva ottenuto la vittoria contro Al Gore per uno stacco di 1784 voti. Lo scarto tra Bush e Al Gore era meno dello 0.5% perciò in base alla legge federale della Florida venne richiesto un riconteggio dei voti a macchina. In seguito al riconteggio, il margine fu ancora più ristretto poiché la differenza tra Bush e Al Gore era pari a 327 voti. Al Gore chiese anche un riconteggio manuale nelle contee di Volusia, Palm Beach, Broward e Miami – Dade. Si giunse alla Corte Suprema degli Stati Uniti la quale ammise la richiesta di Al Gore, anche se l'orientamento non fu favorevole al riconteggio manuale in quanto avrebbe violato la *Equal Protection Clause* prevista dal quattordicesimo emendamento mettendo in luce, inoltre, che gli standard per il conteggio manuale variano da contea a contea, perciò gli elettori non potevano essere certi che i loro voti fossero conteggiati. Si veda https://edition.cnn.com/2000/ALLPOLITICS/stories/11/15/jackson.punchcards/;https://supreme.justia.com/cases/federal/us/531/98/.

[447] Ahmad, Tabassum, Ayaz, Bahir, & Meelam, 2021

[448] *Ibidem*

[449] In breve si tratta del software utilizzato nei macchinari per il voto elettronico negli Stati Uniti, il quale funziona tramite l'inserimento da parte dell'elettore di una smartcard a seguito del quale compare sullo schermo del macchinario la scheda elettorale e l'elettore può esprimere la propria preferenza. La discussione attorno al sistema di Diebold risiede su due punti principalmente, ossia la smartcard e il codice sorgente chiuso, il quale non consente di verificare la presenza di eventuali bug del sistema. La problematica più rilevante, però, riguarda la smartcard, in quanto l'elettore, una volta espressa la propria preferenza, doveva restituirla al pubblico ufficiale, il quale la riprogrammava. Su questo versante sono evidenti i rischi connessi alla sicurezza, in quanto era possibile l'introduzione alle rune di smartcard fasulle che registrasse la procedura di riprogrammazione. Inoltre, a seguito della procedura di voto la smart card viene disattivata e un abile informatico non avrebbe alcun problema nel riprogrammare la card se è in grado di risalire al codice sorgente, seppur chiuso, del software. Per ulteriori informazioni si veda Awad & Leiss, 2016

[450] Sciannella, 2020

presidiata esso si presenta come una modalità di votazione integrativa o esclusiva attraverso la quale il voto "*viene reso dall'elettore in postazioni sorvegliate da pubblici ufficiali*"[451]. Si può pacificamente affermare, quindi, come questo approccio alla votazione non sia nient'altro che un aggiornamento della modalità tradizionale, poiché permane per gli elettori l'obbligo di recarsi alle urne. Nel voto elettronico presidiato, difatti, ciò che cambia è il mezzo attraverso il quale gli elettori esprimono la loro preferenza, ossia anziché utilizzare la scheda elettorale cartacea e la matita copiativa viene impiegato un dispositivo elettronico. Il voto nella forma presidiata, inoltre, garantisce una maggior corrispondenza tra la volontà dell'elettore e quanto espresso nella scheda elettorale digitale. Difatti, se con la compilazione della scheda cartacea vi possono essere dei dubbi di carattere interpretativo circa l'apposizione dei segni e della corretta compilazione della scheda, nella modalità elettronica la preferenza viene immediatamente registrata e l'elettore deve attenersi solamente alle opzioni indicate come valide dall'apparato elettronico[452]. I vantaggi[453] dell'*e-voting,* dunque, nella forma presidiata si colgono non nell'immediato ma nella fase successiva, ossia al momento dello scrutinio e dell'elaborazione dei risultati, in quanto chi li conteggerà non sarà il presidente del seggio, il segretario e gli scrutatori, ma il programma adibito al conteggio presente nel macchinario. I vantaggi che tale modalità di espressione del suffragio offre si possono cogliere, invece, nella forma del voto elettronico non presidiato consistente nell'espressione del voto attraverso applicazioni o siti web che rendono agevole l'esercizio di tale diritto, in quanto è possibile esprimere la propria preferenza in qualsiasi momento, in qualsiasi luogo e da qualsiasi device elettronico[454]. Nonostante la evidente comodità fornita da tale forma di votazione permangono delle perplessità sulla sua implementazione nelle democrazie odierne, difatti l'Estonia è l'unico Paese al mondo ad utilizzare tale modalità di votazione con il *Remote Internet Voting*[455]. Le perplessità sorgono soprattutto dal punto di vista della libertà e personalità del voto. In particolare, nell'ordinamento interno si fa riferimento all'articolo 48 della Costituzione, il quale disciplina l'esercizio del diritto al voto. Per quanto attiene alla libertà di voto tale principio afferma che l'elettore deve poter esprimere il proprio suffragio liberamente in assenza di coercizioni esterne. Nel voto elettronico non presidiato non si può escludere che vi siano di coercizioni

[451] Gometz, 2017
[452] *Ibidem*
[453] Tra i molteplici vantaggi offerti dal voto elettronico si ricorda, a titolo di esempio, la comodità per l'elettore il quale non deve necessariamente recarsi alle urne, se si sceglie la modalità non presidiata, nonché una riduzione in termini di costi sia pubblici sia privati. Per costi pubblici si intendono tutte le risorse economiche che lo Stato investe per la predisposizione delle infrastrutture, delle attrezzature e del personale necessario ai fini dell'esercizio del diritto di voto, mentre i costi privati riguardano le risorse dei privati cittadini economiche e non che vengono utilizzate affinché possano esercitare il loro suffragio. A tal proposito si veda Gometz, 2017
[454] Gometz, 2017
[455] Non è detto che il voto attraverso Internet sia necessariamente nella forma non presidiata, in quanto anche alle urne, quindi nella modalità presidiata, vi potrebbe essere l'utilizzo di macchinari collegati ad Internet per la registrazione e il conteggio dei voti.

o pressioni esterne, tali per cui l'elettore non esprime la propria volontà di maniera genuina. Nella modalità non presidiata vi è il rischio per cui l'elettore potrebbe essere soggetto a coercizioni o pressioni esterne, poiché la sua preferenza di voto avviene in luoghi in cui è assente il controllo da parte di pubblici ufficiali e dunque il rischio di corrompere la volontà dell'elettore è più elevato. È un impasse a cui oggi non sembra essere presente una soluzione[456] adeguata, in quanto vi è la difficoltà di effettuare un bilanciamento tra i vantaggi offerti dalla modalità non presidiata e il rispetto della libertà di voto. Da un lato, infatti, nella modalità non presidiata è possibile cogliere i vantaggi del voto elettronico soprattutto in termini di comodità per l'elettore il quale non deve recarsi alle urne e può votare da qualsiasi luogo e in qualsiasi momento. Questa comodità, però, sconta il limite o, meglio, il rischio che la preferenza espressa non sia propriamente genuina. Per quanto riguarda l'aspetto della personalità del voto, il quale è un principio secondo cui il voto deve essere espresso personalmente dall'elettore senza la possibilità del cc.dd. voto per procura[457] sorge qualche perplessità, in quanto potrebbero verificarsi le più svariate circostanze. L'identificazione dell'elettore nella modalità non presidiata avviene principalmente attraverso sistemi digitali come l'utilizzo di *Smart Card* ed emblematico è il caso dell'Estonia oppure tramite dati biometrici come la scansione del volto o l'utilizzo delle impronte digitali. In questo frangente potrebbe sorgere qualche criticità. L'elettore, per esempio, potrebbe perdere le proprie credenziali oppure si potrebbero verificare dei furti d'identità. Ad esempio, l'elettore si autentica al portale di votazione elettronica con le proprie credenziali, ma di fatto colui che esercita il diritto al voto è un altro individuo, il quale potrebbe esprimere un voto che non combacia con la volontà dell'elettore oppure addirittura potrebbe essere un soggetto privo dei requisiti necessari per far parte dell'elettorato attivo[458]. Sono tutte situazioni limite, ma che potrebbero nel concreto verificarsi. Alla luce di queste brevi riflessioni è possibile constatare come il tema del voto elettronico sia un tema scottante e come, al momento, nonostante gli indubbi vantaggi siano ancora presenti alcune perplessità circa il suo impiego soprattutto se si intende implementare la forma non presidiata.

[456] Ad esempio, l'Estonia è l'unico Paese al mondo ad utilizzare in tutte le elezioni, nazionali ed europee, il *Remote Internet Voting* ossia una forma di voto elettronico non presidiato consentendo agli elettori di esprimere la loro preferenza più volte sulla piattaforma digitale, annullando quella precedente. Nel caso in cui non fossero convinti del voto espresso in modalità elettronica, gli elettori al giorno delle elezioni possono rivolgersi alle urne e votare secondo le modalità tradizionali annullando il voto espresso in via digitale. È una delle soluzioni proposte per ammettere il voto elettronico non presidiato e superare l'impasse con il principio di libertà del voto.

[457] Circostanza per la quale l'elettore delega un altro soggetto, affinché eserciti il suo diritto al voto.

[458] Per elettorato attivo si fa riferimento alla capacità di votare. Per poter esercitare il diritto al voto è necessario essere cittadini italiani e aver raggiunto la maggiore età. Il comma quarto dell'art.48 Cost. prevede, poi, dei requisiti negativi, ossia "*il diritto al voto non può essere limitato se non per incapacità civile o per effetto di sentenza penale irrevocabile o nei casi di indegnità morale indicati dalla legge".*

2. Blockchain applicate al voto elettronico

Dopo aver brevemente illustrato il concetto di voto elettronico e preso atto della difficoltà di inquadrare il fenomeno in maniera univoca, nei prossimi paragrafi verrà studiato l'utilizzo delle tecnologie blockchain nell'ambito dell'*e-voting*. Le ragioni per cui si indaga questo tema traggono origine dalle riflessioni effettuate circa la democrazia elettronica e l'esercizio del diritto al voto attraverso una modalità alternativa quale quella del voto elettronico che ancora oggi pone numerose sfide alle democrazie odierne intenzionate a sperimentare tale modalità di espressione del suffragio per cercare di porre un freno al crescente astensionismo degli elettori e rinnovare l'interesse per la politica. La trattazione proseguirà in tal senso: in un primo momento verrà descritto il funzionamento delle blockchain nel voto elettronico per, poi, passare allo studio circa la compatibilità o meno di tali tecnologie con i principi espressi in materia e infine verrà illustrato il funzionamento di alcune delle piattaforme di votazione elettronica su blockchain più diffuse e conosciute nel settore.

2.1. Come funzionano le blockchain nel voto elettronico

Nel precedente paragrafo si è cercato di dare una definizione di voto elettronico concentrandosi sull'evoluzione tecnologica dei sistemi di votazione digitale nonché sulla modalità con cui il suffragio può essere espresso, ossia in forma presidiata o non presidiata. Sono indubbi gli aspetti positivi del voto elettronico come, ad esempio, la possibilità di votare in qualsiasi luogo e in qualsiasi momento[459], ma altrettanto sono evidenti le difficoltà di implementazione di tale sistema, come il difficile coordinamento tra voto elettronico e principi generali in materia, di cui si dirà poco più avanti, e la sicurezza dei sistemi di votazione elettronica. Per quanto attiene a quest'ultimo profilo, il concetto di sicurezza assume diverse sfumature di significato, in quanto si riferisce sia alla necessità di verificare, da parte dell'elettore, che la sua volontà sia corrispondente a quanto espresso nella scheda elettorale sia ad evitare che siano presenti eventuali malfunzionamenti del sistema che portano a possibili brogli, alterazioni o interferenze tali per cui vi è una manipolazione dei risultati[460]. Si possono, pertanto, verificare alcune situazioni in cui la sicurezza delle piattaforme di votazione venga meno, in quanto vittima di attacchi informatici. Difatti, per quanto si implementino e aggiornino i sistemi di sicurezza informatica, non è possibile garantire un livello di sicurezza *tout court* a causa degli sviluppi e della

[459] Facendo riferimento al voto elettronico non presidiato.
[460] Gometz & Tawa , 2018

presenza di nuove forme di aggressione[461]. In questo frangente, dunque, si inserisce lo studio di una possibile applicazione della tecnologia blockchain nel voto elettronico per porre rimedio ai problemi attinenti alla sicurezza dei sistemi di votazione digitale. Dal punto di vista applicativo, considerare l'impiego della tecnologia blockchain al voto elettronico implica effettuare una serie di valutazioni attinenti a vari componenti base di tale tecnologia che influenzano l'intero sistema di votazione. La prima scelta da effettuare concerne l'algoritmo di consenso, ossia le regole a cui i nodi della rete devono sottostare per la creazione e la validazione di un nuovo blocco[462]. Questa scelta è cruciale, in quanto influenza il cc.dd. problema della scalabilità consistente nella capacità della rete di gestire un numero sempre più elevato di transazioni garantendo all'aumento di esse l'efficienza e la sicurezza che contraddistingue questa tecnologia[463]. A seconda, poi, del protocollo di consenso adottato, deriva un ulteriore aspetto della blockchain ossia la sua robustezza, detta altrimenti resilienza agli attacchi informatici[464] per cui vi possono essere differenti livelli di sicurezza della rete. Strettamente correlato a questo aspetto vi è la seconda considerazione che riguarda la tipologia di blockchain[465] scelta per l'operazione elettorale. Qualora si optasse per una blockchain pubblica, detta *permissionless,* tra i nodi della rete vi è un grado di fiducia molto basso in quanto si tratta di una rete pubblica accessibile a tutti. Il vantaggio della blockchain *permissionless* consta nel fatto che più la rete è estesa, più è sicura per cui anche in presenza di un attacco informatico l'intero sistema continua a funzionare, in quanto i nodi

[461] Tra le aggressioni informatiche più comuni in materia di sicurezza digitale si può far riferimento al cc.dd. *data breach,* ossia un attacco informatico perpetrato da un hacker con l'obiettivo di ottenere un accesso non autorizzato al rilascio e alla diffusione di dati sensibili. Un'altra tipologia di attacco molto comune è il *Distributed Denial of Service,* indicato con l'acronimo DDoS, il quale impedisce agli utenti di un servizio, come nel caso del voto elettronico, o di un sistema ad avere accesso ai dati, adi servizi o ad altre risorse. Il DDoS viene realizzato attraverso un sovraccarico dell'infrastruttura di rete esaurendo così il servizio e le sue risorse. Infine si ricorda l'Internet shutdown, ossia il blocco di Internet consistente in una sospensione volontaria del servizio di Rete o delle comunicazioni rendendole inaccessibili o utilizzabili in riferimento ad una specifica popolazione o località con lo scopo di effettuare un controllo sulla diffusione delle informazioni. Per ulteriori informazioni sugli attacchi informatici, la loro diffusione e le tendenze si veda https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[462] Ul Abadin & Haider Syed , 7th July 2021

[463] Ad esempio, l'algoritmo di consenso maggiormente conosciuto e diffuso è il Proof of Work, il quale richiede ai nodi della catena di risolvere un complesso puzzle matematico sfruttando il proprio potere computazionale affinché possano aggiungere un nuovo blocco alla catena. È evidente che più i problemi matematici sono complessi, più sarà il tempo necessario per risolverli pertanto ciò comporta ad una riduzione del numero di transazioni validate all'interno della catena. Tendenzialmente, il Proof of Work utilizzato nel Bitcoin effettua una transazione ogni dieci minuti, un valore molto basso rispetto alla media. Ad esempio, Ethereum esegue una transazione ogni 6,4 minuti. Per ulteriori informazioni si veda https://ethereum.org/it/roadmap/merge/issuance/#cl-issuance-post-merge e https://ultrasound.money/.

[464] Tra gli attacchi informatici più comuni che colpiscono la rete blockchain si può ricordare il Double spending problem, ossia la circostanza per la quale un soggetto cerca di spendere un ammontare di denaro nella blockchain per due volte cercando di includere un nuovo blocco nella rete creando una transazione fraudolenta. Altro attacco molto comune è il cc.dd. 51% attack, ossia colui che attacca la rete blockchain è in grado di controllarne più del 50% ed è in grado, dunque, di effettuare alcune operazioni malevoli come impedire ad altri nodi di ricevere transazioni oneste. Infine vi è il Sybil attack per cui si cerca di controllare la rete creando un numero non ben definito di identità, ossia utenti, fraudolente nella blockchain. Mojtaba , Bamakan , Motavali, & Babei Bondarti , 13th April 2020

[465] Per completezza, si deve ricordare anche le cc.dd. blockchain consortium le quali uniscono elementi della blockchain pubblica e della blockchain privata. La più famosa è Aura Blockchain impiegata nel settore del luxury per evitare contraffazioni e per garantire la tracciabilità del prodotto. Per ulteriori informazioni https://auraconsortium.com/about

rimanenti detengono una copia dei dati della rete pertanto fungono da backup. Nel settore elettorale la blockchain pubblica risulta essere appetibile, in quanto presenta una struttura fortemente decentralizzata, dunque priva di un soggetto terzo che funge da intermediario a differenza della blockchain privata o *permisisoned.* Nonostante le caratteristiche dell'assenza di intermediari e dell'anonimato garantite da tale tecnologia possano essere allettanti per l'utilizzo della tecnologia blockchain nel settore elettorale, è da rilevare come possano avere anche un risvolto negativo, poiché vi potrebbe essere un utilizzo malevolo tale per cui non si esclude lo scambio di voti per denaro. Difatti, la possibilità di utilizzi malevoli è sempre presente poiché si tratta di una rete aperta a tutti, per cui chiunque vi può partecipare, oltre al fatto che l'anonimato rende difficile risalire all'identità di colui che ha eseguito la transazione, anche se l'analisi dei dati permetterebbe di scoprire determinati pattern comportamentali e risalire così all'identità delle parti coinvolte nell'operazione[466]. Vista la portata del diritto al voto e tutto ciò che esso implica e il rischio che la rete *permissionless* possa essere utilizzata per fini malevoli, la blockchain *permissioned,* detta altrimenti privata, sembrerebbe essere la più adeguata al settore elettorale. Tale tipologia di blockchain, infatti, prevede un elevato grado di fiducia tra i nodi, dal momento che i *peers* nella rete sono in quantità nettamente inferiore rispetto alla blockchain pubblica presentando, dunque, una struttura più centralizzata. Nelle blockchain *permissioned* per poter far parte della rete è necessario ottenere l'autorizzazione da parte di un'autorità a ciò preposta[467], la quale funge da *cancello d'ingresso*, per cui per partecipare alla rete vi deve essere la soddisfazione di alcuni criteri richiesti dalla blockchain stessa. In questo caso, ci si pone in una situazione inversa rispetto alla precedente, in quanto non essendoci una rete estesa vi è un maggior rischio di essere vittima di attacchi, ma allo stesso tempo vi è un maggior grado di fiducia tra le parti. Ulteriore tassello che consente di progettare un sistema di votazione che sfrutti le blockchain consiste nel rispetto di alcuni requisiti, affinché vi possa essere un sistema che garantisca elezioni trasparenti e sicure. In letteratura si concorda circa su almeno tre requisiti necessari, ossia (i) anonimato, (ii) sicurezza e (iii) verificabilità. Per quanto riguarda l'anonimato, nella tecnologia blockchain ciò è garantito dal fatto che l'identità dei partecipanti alla rete non è resa nota e pertanto non è possibile risalire agli autori delle transazioni. Nel voto elettronico, l'utilizzo della blockchain assicura l'impossibilità di associare la preferenza espressa all'elettore, per cui la sua identità rimane nascosta essendo le sue informazioni contenute in un valore di hash unico e univoco per ciascun partecipante alla rete[468]. La funzione di hash, infatti, è una delle tecniche di crittografia più utilizzate e affidabili, in quanto ad un determinato *imput* corrisponde un *output* unico nel suo genere, tale per cui in caso di

[466] Bayan & Banach , 4-6 May 2023
[467] Yaga, Mell, Roby, & Scarfone, 2018
[468] Tasmia Alvi , Nasir Uddin, Islam, & Ahame, 2022

eventuale modifica essa è immediatamente visibile in quanto vi è l'emissione di un *output* diverso rispetto a quello di partenza. Ulteriore elemento che deve essere garantito dalla blockchain nel settore elettorale e da cui è partita la riflessione sul tema è la sicurezza. In generale essa si rispecchia nella caratteristica dell'immutabilità, tale per cui una volta effettuata una transazione il blocco appena creato e inserito all'interno della catena non può essere più modificato. Pertanto, qualora dovesse esserci un attacco informatico, ciò sarebbe immediatamente visibile. A dire del vero, nonostante la sicurezza sia una delle prerogative della tecnologia blockchain garantita dalla caratteristica dell'immutabilità e dai sistemi di crittografia è altrettanto chiaro come la rete blockchain, come ogni tecnologia, non sia immune da aggressioni informatiche. Sul punto è emblematica la vicenda di *ChildDao*[469]*,* un attacco hacker perpetrato sulla blockchain Ethereum. In breve, nel 2016 la piattaforma inaugurò *The DAO*, acronimo per *Decentralised Autonomous Organisation,* un fondo autonomo di investimenti che nel suo breve periodo di vita riuscì a raccogliere più di 150 milioni di dollari. A luglio del 2016, un hacker sfruttando un errore di programmazione del codice consistente nella *split function* riuscì a prelevare lo stesso ammontare di Ether più volte prima che la blockchain potesse elaborare la transazione. Una volta scoperto l'arcano, i progettisti di Ethereum optarono per l'*hard fork,* ossia una soluzione consistente nel cambio delle regole di validazione dei blocchi consistente in un mutamento del protocollo di consenso. Con l'*hard fork,* quindi i blocchi che sono stati validati seguendo le regole precedenti non vengono considerati dai nodi che utilizzano le nuove regole di validazione come validi e aggiunti, quindi, alla catena. Infine, ulteriore elemento è la verificabilità detta anche *audit* che si traduce nel principio di trasparenza per cui tutti i dati della blockchain devono essere accessibili per verificare se il voto espresso dall'elettore sia stato inserito correttamente nella rete. La verificabilità può essere universale, ossia chiunque può effettuare tale operazione oppure individuale, per cui solo colui o colei che ha espresso il voto può controllare in concreto se la procedura si sia conclusa correttamente[470]. Poste le basi per la creazione di un sistema di votazione digitale su blockchain è possibile descriverne il funzionamento nell'ambito oggetto di analisi. Tradizionalmente il settore di impiego della blockchain è quello finanziario nel quale vi è uno scambio di denaro, ossia criptovalute come il Bitcoin. Tale operazione di scambio avviene attraverso una transazione all'esito della quale un nuovo blocco viene aggiunto alla catena. Lo stesso lo si può dire per il voto. Nell'architettura della tecnologia blockchain, infatti, anche il voto assume le sembianze di una transazione in quanto implica uno scambio. Tale scambio anziché avere ad oggetto una somma di denaro, presenta come oggetto l'espressione della preferenza dell'elettore per un determinato partito e/o candidato. Riprendendo,

[469] Per riprendere la vicenda si veda https://medium.com/@jordans2299/revisiting-the-dao-hack-33224d641303.
[470] Tasmia Alvi , Nasir Uddin, Islam, & Ahame, 2022

quindi, il concetto di blockchain si può descrivere il suo funzionamento come una catena di blocchi collegati tra di loro attraverso il richiamo al valore di hash del blocco precedente nel blocco successivo. Nel momento in cui si verifica una transazione e questa è eseguita correttamente, il nuovo blocco viene aggiunto alla catena, ma prima della sua aggiunta deve essere approvato da tutti i *peers,* ossia i nodi, della rete[471]. Tale approvazione avviene seguendo le regole del protocollo di consenso adottato. Vista la particolarità del suo utilizzo, vi possono essere delle modifiche allo schema generale per adeguarlo alle esigenze che pone il settore elettorale come, ad esempio, garantire un certo livello di sicurezza del sistema a presidio della consultazione elettorale e della democraticità della procedura stessa, nonché assicurarsi che tutti gli aventi diritto al voto che decidano di sfruttare il voto elettronico vengano correttamente identificati dai sistemi digitali per assicurare elezioni trasparenti e per evitare che si verifichino episodi di voti comprati, rubati o estorti[472]. Nel caso di specie, in letteratura si è individuato uno schema generale che riguarda le consultazioni elettorali, il quale prevede l'utilizzo di *smart contracts* che sfruttano principalmente le reti blockchain di Ethereum e di Hyperledger Fabric, ossia su blockchain *permissioned,* per garantire una maggior privacy e sicurezza, nonché per evitare il problema della scalabilità. A tal proposito si può citare come esempio, il sistema progettato da Soud, Helgason, Hjàlmtysson e Hamdaqa, ossia TrustVote[473]. L'obiettivo di TrustVote è di carattere manageriale, in quanto intende semplificare la gestione della votazione elettronica e ridurre gli errori umani. La caratteristica che distingue TrustVote rispetto ad altre proposte in letteratura consiste nel fatto che all'interno della sua architettura sono presenti due tipologie di nodi, ossia i *managerial nodes* e i *district nodes.* I primi hanno come compito quello di gestire il sistema e assicurarne l'integrità, mentre i secondi rappresentano nel mondo digitale ciò che nel mondo reale sono i distretti elettorali. Ogni distretto, quindi, è in grado di interagire con la rete e ha il compito di gestire gli *smart contract* ad esso collegati[474]. Per quanto attiene alla consultazione elettorale, essa viene considerata come una serie di transazioni concatenate tra loro. Il primo passaggio consiste nella predisposizione da parte degli *election administrators*[475] dell'*Election Creation Smart Contract*[476], il quale contiene la lista dei candidati e dei distretti elettorali. In questa fase preparatoria viene predisposto anche il *Ballot Smart Contract,* contente solo la lista dei candidati. Nella fase successiva entrano in gioco gli elettori, i quali vengono registrati e autorizzati dal sistema di verificazione prescelto. Ogni elettore riceverà il proprio ID, PIN, distretto elettorale di appartenenza e OTP, ossia *one time password* che può essere utilizzata

[471] Faini, 2020
[472] Benabdallah , Audras , Coudert , El Madhoun , & Badra , 2022
[473] Soud , Helgason, Hjálmtýsson, & Hamdaqa, 2020
[474] *Ibidem*
[475] Sono i soggetti preposti a dare avvio alla consultazione elettorale specificando il tipo di elezione, la durata e assegnare i nodi autorizzati a far parte della rete.
[476] Abbreviato in ECSC.

per recuperare i propri dati. A seguito dell'autenticazione, all'elettore viene trasmessa la scheda elettorale e il suffragio viene espresso tramite l'ausilio di un computer presente nel seggio del distretto di appartenenza. Si tratta, dunque, di una forma di voto elettronico presidiato. Una volta espressa la propria preferenza, il voto viene verificato dal *district node* e il consenso è raggiunto solo quando la maggioranza dei *district node* concordano sulla correttezza dei dati afferenti al voto. Una volta raggiunto il consenso, il blocco viene aggiunto alla catena. Una volta registrati tutti i voti, alla chiusura della elezioni vi è il conteggio dei voti, operazione che viene effettuata dal *Ballot Smart Contract,* il quale pubblica i risultati finali per il proprio distretto di appartenenza. Infine, il sistema invia un *transaction ID* all'elettore cosicché può verificare se il proprio voto sia stato registrato correttamente, in ossequio allo standard della verificabilità. Alla luce di questo esempio, si possono individuare le fasi principali attinenti alla procedura di votazione. In primis, vi è la inizializzazione che, se nella modalità tradizionale consiste nella preparazione dei seggi, nella modalità elettronica tale fase consiste nella predisposizione degli *smart contract* i quali stabiliscono le regole per la votazione, la lista degli elettori aggiornata e la lista dei candidati[477]. Una volta conclusa la fase preparatoria, vi è l'autenticazione degli elettori. Nella modalità tradizionale avviene un tramite un documento, come la carta d'identità o la patente di guida, mentre per il voto elettronico sono previsti diversi meccanismi di identificazione. Per quanto attiene alla blockchain, il meccanismo prediletto è l'identificazione tramite la creazione di una coppia di chiavi pubbliche e private[478] le quali fungono da password che consentono agli utenti di accedere alla blockchain e di effettuare le transazioni all'interno della rete. Non si esclude, però, l'utilizzo di altri sistemi di identificazione come l'impiego di dati biometrici quali le impronte digitali e la scansione del viso spesso combinati con un ulteriore elemento identificativo dando vita, quindi, all'identificazione multi-fattore[479]. Successivamente, l'elettore può esprimere la propria preferenza tra una rosa di candidati e una volta che la sua preferenza è stata espressa e registrata, il voto viene crittografato seguendo le regole della blockchain attraverso diverse tecniche di crittografazione, tra cui le funzioni di hash. Nella modalità analogica, invece, l'elettore una volta manifestata la sua preferenza semplicemente inserisce la scheda elettorale all'interno dell'urna dinnanzi al presidente del seggio e agli scrutatori. La fase finale prevede il conteggio dei voti e la pubblicazione dei risultati. È chiaro come nella modalità tradizionale di votazione tale fase sia più lunga e laboriosa che richiede anche un elevato grado di attenzione[480], mentre nel voto elettronico, grazie al supporto informatico è possibile

[477] Benabdallah , Audras , Coudert , El Madhoun , & Badra, 2022
[478] *Ibidem*
[479] Per approfondire si guardi Hossain Faruk, Aman , Islam , & Rahman, 2024
[480]Mi riferisco al fatto che il conteggio avviene per opera degli scrutatori e del presidente del seggio ed è un'operazione che richiede un elevato grado di attenzione. Difatti, oltre al semplice aprire e contare le schede elettorali, è necessario aver presente tutte le regole attinenti alla corretta compilazione della scheda e quando essa viene considerata nulla.

eseguire tali operazioni in tempi più brevi. In particolare, qualora vi fosse l'utilizzo degli *smart contracts* durante le consultazioni elettorali essi avrebbero il compito, se predisposti, di conteggiare i voti e di pubblicare i risultati come avviene nel caso di TrustVote con il *Ballot Smart Contract*. Alla luce di questa breve panoramica sul funzionamento della blockchain nel voto elettronico è possibile affermare come tale tecnologia possa trovare applicazione in questo settore, poiché l'espressione del suffragio e la consultazione elettorale si traducono in una serie di transazioni seguendo, dunque, lo schema generale di funzionamento della blockchain ferma restando la possibilità di usufruire degli *smart contracts* come si è visto con TrustVote. Inoltre si evince come è la blockchain che deve adattarsi al voto elettronico e non viceversa, in quanto è la tecnologia alla base sfruttata per le consultazioni elettorali, tale per cui è necessario effettuare alcune scelte, come il protocollo di consenso e la tipologia di rete, che si rivelano strategiche in questo settore considerata la portata dell'esercizio del diritto al voto non solo dal punto di vista strettamente tecnico, ma anche dal punto di vista politico – giuridico incidendo notevolmente sulla democraticità del sistema. Nel prossimo paragrafo verrà approfondito l'aspetto della compatibilità tra la tecnologia blockchain e i principi espressi in materia elettorale sia a livello della legislazione interazionale sia a livello interno con particolare riferimento all'art.48 Cost. e ai principi di personalità, eguaglianza, libertà e segretezza del voto.

2.2. Blockchain e voto: compatibilità con i principi internazionali in materia elettorale e con l'art.48 Cost.

Prima di analizzare alcuni esempi di utilizzo della tecnologia blockchain nel voto elettronico è opportuno soffermarsi sulla eventuale compatibilità o meno di tale tecnologia con i principi espressi in materia sia da un punto di vista più ampio, ossia quello internazionale, sia dalla prospettiva interna con riferimento all'articolo 48 della Costituzione.

2.2.1. Blockchain e le Raccomandazioni del Consiglio d'Europa

Si potrebbe tratteggiare una linea temporale di quelle che sono state le pietre miliari a livello internazionale circa l'esercizio del diritto al voto, ma per quanto attiene alla compatibilità tra voto e blockchain ci si sofferma sulle Raccomandazioni del Consiglio d'Europa del 2004 e del 2017, in quanto sono i testi che riguardano nello specifico il voto elettronico. È interessante osservare come il testo del 2004 sia molto più ampio e dettagliato rispetto alla versione aggiornata del 2017, segno che agli inizi degli anni 2000 nel pieno della Internet Revolution la discussione circa l'utilizzo di supporti informatici nelle consultazioni elettorali era particolarmente sentita. Nonostante il testo del 2004 sia più dettagliato c'è da considerare, però, che alla Raccomandazione del 2017 è allegato un

memorandum esplicativo, ossia un testo aggiuntivo che in riferimento ai singoli punti della Raccomandazione provvede ulteriori spiegazioni e precisazioni. Nel preambolo della Raccomandazione del 2004, come accennato poc'anzi, si prende atto di come il voto elettronico possa essere utilizzato per diversi fini tra cui facilitare la partecipazione dei cittadini nei processi elettorali ed essere al passo con il mutare dei costumi della società dovuti anche all'utilizzo di nuove tecnologie nell'ambito della comunicazione e partecipazione civica. I principi a cui il voto elettronico deve sottostare sono (i) l'universalità del suffragio, (ii) la libertà del suffragio e la (iii) la segretezza del voto[481]. L'universalità del suffragio viene considerata dal punto di vista dell'accessibilità, per cui tutti i cittadini devono poter usufruire dei servizi di votazione elettronica nel rispetto dei limiti posti dall'ordinamento interno quali, ad esempio, l'età per poter votare e soddisfare il requisito della cittadinanza. All'interno dell'universalità del suffragio viene considerato anche il principio di uguaglianza intenso nel senso di evitare il cc.dd. voto multiplo tale per cui un elettore vota *n-volte* violando, di conseguenza, il principio *una testa un voto*[482]. Per quanto attiene, invece, alla libertà del suffragio l'obiettivo è quello di tutelare la libertà di voto nel senso di garantire tutte le condizioni necessarie affinché l'elettore possa esprimere la propria preferenza in assenza di coercizioni esterne. Ulteriore aspetto di tale principio riguarda la facoltà per l'elettore di cambiare idea prima dell'invio al sistema di votazione elettronica della propria preferenza o attraverso un'interruzione della procedura prima che la sua scelta venga registrata. Da questo punto di vista, la tecnologia blockchain risulterebbe essere non compatibile con quello che è il principio di libertà inteso come "diritto di sbagliare". Una volta avviato il procedimento di votazione, infatti, nella blockchain viene avviata una transazione, la quale non può essere interrotta. Una soluzione prospettabile sarebbe quella di utilizzare algoritmi di consenso progettati *ad hoc* che consentano all'elettore di riconsiderare la propria scelta. Il tutto, quindi, dipende da come viene progettato il sistema di votazione elettronica e dalle eventuali considerazioni effettuate in riferimento a varie questioni che la consultazione elettorale pone[483]. Infine, per quanto attiene alla segretezza del voto nella Raccomandazione del 2004 l'obiettivo perseguito è quello di

[481] Il testo della Raccomandazione del 2004 è molto ampio e prevede anche una parte dedicata alle garanzie di carattere procedurale come la trasparenza e la verificabilità, nonché prevede una serie dettagliata di standard a cui i sistemi di votazione elettronica devono sottostare, soprattutto dal punto di vista tecnico. Ai fini della trattazione, però, si considerano solo i principi generali espressi in materia. Per ulteriori approfondimenti si veda: https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp

[482] Nel testo originale della Raccomandazione del 2004 al punto 5 viene asserito "*[…] a voter shall be prevented from inserting more than one ballot into the electronic ballot box"* e al punto 6 "*The e-voting system shall prevent any voter form casting a vote by more than one voting channel".* Tradotto, l'elettore non può inserire il suo voto per più di una volta nell'urna elettronica e il sistema di votazione deve impedire la circostanza per la quale l'elettore possa votare più volte usufruendo di diversi canali di votazione.

[483] Mi riferisco, ad esempio, all'aspetto della sicurezza dei sistemi informatici utilizzati e alle adeguate misure di sicurezza che devono essere adottate per garantire elezioni sicure e trasparenti o ancora alla tipologia di consultazione elettronica, ossia se in forma presidiata o non presidiata oppure alle singole fasi del procedimento elettorale e la scelta in quale di esse considerare o meno l'utilizzo di supporti informatici etc.

evitare che al voto espresso si possa risalire all'identità di colui o colei che lo ha espresso. Dal punto di vista della blockchain, questo standard è rispettato in quanto tutte le transazioni effettuate nella rete sono anonime a tutela la privacy dei partecipanti alla rete. Facendo, poi, un confronto con la Raccomandazione del 2017 in essa vengono considerati gli stessi principi, seppur in termini leggermente diversi. A tal proposito, per esempio, in riferimento all'uguaglianza del voto allo standard n.7 viene previsto ciò che nel nostro ordinamento è il principio di personalità. In particolare la Raccomandazione fa riferimento ad un' identificazione univoca degli elettori in modo che possano essere distinti da altri soggetti senza alcun margine di errore[484]. Nel memorandum esplicativo si precisa che per identificazione univoca si fa riferimento alla procedura per la quale l'identità di una persona viene autenticata attraverso il riconoscimento di una o più caratteristiche affinché possa essere riconosciuta distintamente da tutte le altre[485]. Per quanto attiene, invece, alla libertà di voto la Raccomandazione del 2017 risulta essere più attenta su questo aspetto rispetto al precedente testo adottato. Per libertà di voto si fa sempre riferimento alla circostanza per cui l'elettore deve essere in grado di poter esprimere la propria preferenza in assenza di coercizioni esterne e, in particolare, lo standard n.15 prevede "*The voter shall be able to verify that his or her intention is accurately representend in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable"* e ancora allo standard n.16 "*The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting process has been completed".* Su questo punto, quindi, la libertà di voto si traduce nella verificabilità, ossia l'elettore deve essere in grado di appurare che la sua volontà sia corrispondente a quanto espresso nella scheda elettorale e che il voto così manifestato sia correttamente inserito nell'urna digitale senza essere alterato. Ogni eventuale tentativo di modificazione del suffragio deve essere, quindi, immediatamente visibile. Inoltre la libertà di voto si traduce anche in un principio di certezza, ossia l'elettore deve essere sicuro che il suo voto sia stato registrato correttamente e che l'intero procedimento di votazione sia completato. La tecnologia blockchain soddisfa tale esigenza, in quanto grazie alla sua caratteristica dell'immutabilità sono immediatamente visibili eventuali tentativi di alterazione delle transazioni avvenute. Infine, ulteriore differenza rispetto al testo del 2004 riguarda il principio di uguaglianza. Se nella Raccomandazione precedentemente adottata per uguaglianza si intende evitare il voto multiplo, nel testo del 2017 uguaglianza fa riferimento all'uguaglianza di contenuto considerati i diversi canali di votazione, ossia cartaceo ed elettronico, tali per cui è

[484] Il testo originale della Raccomandazione recita allo standard n.7 "*Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured".*
[485] Si veda *Memorandum esplicativo 14 giugno 2017* punto n.41
https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84

necessario che l'elettore abbia adeguate informazioni per entrambi[486]. In generale, quindi, si può affermare che la tecnologia blockchain per quanto riguarda le linee guida previste dalle Raccomandazioni summenzionate sia compatibile con i principi espressi in materia, seppur con qualche limite come, ad esempio, in riferimento al principio di libertà e il "diritto", per così dire, dell'elettore a sbagliare e a cambiare idea ed esprimere una preferenza diversa rispetto a quella di partenza.

2.2.2. Blockchain e l'art.48 Cost.

Nel precedente paragrafo si è analizzata in breve la compatibilità tra i principi espressi dalle Raccomandazioni del 2004 e del 2017 del Consiglio d'Europa mettendone in luce le differenze osservando come la tecnologia blockchain possa essere compatibile con i principi espressi dai summenzionati testi, seppur con qualche limite. Per quanto riguarda, invece, la compatibilità tra blockchain e i principi costituzionali l'articolo 48 è il punto a cui fare riferimento. Vi è, però, una considerazione da effettuare. Qualora si volesse nell'ordinamento interno sperimentare l'utilizzo del voto elettronico[487] è fondamentale tener presente che i principi di personalità, uguaglianza, libertà e segretezza sono irrinunciabili per l'ordinamento pertanto non sarebbero suscettibili di eventuali attenuazioni. Questa rigidità è a presidio dell'esercizio del diritto al voto, ossia una delle forme, se non la forma, più rilevante con cui si esprime la sovranità del popolo colonna portante di ogni democrazia che trae origine dalle vicissitudini che hanno colpito il Paese tra gli anni '20 e '40 del secolo scorso. Difatti, dottrina costituzionale consolidata prevede una lettura congiunta dell'articolo 1 della Costituzione e dell'articolo 48, soprattutto in riferimento all'aspetto del suffragio universale[488]. Generalmente, nell'articolo 48 possono essere individuate due coppie di garanzie fondamentali, ossia da un lato la personalità e l'uguaglianza e dall'altro la libertà e segretezza, in quanto l'uno strettamente correlato all'altro. Per quanto riguarda il principio di personalità[489], esso richiede che il voto debba

[486] Si veda *Memorandum esplicativo 14 giugno 2017* punto n.37

[487] Mi riferisco in particolare alla legge di bilancio del 2020 n.160/2019 la quale ha previsto lo stanziamento di alcuni fondi per la sperimentazione del voto elettronico per le elezioni politiche ed europee e per i referendum previsti dagli articoli 75 e 138 della Costituzione il cui utilizzo è stato descritto con il decreto ministeriale del 9 luglio 2021.

[488] È assai noto come il suffragio universale sia solo una recente conquista avvenuta con la Costituzione del 1948. Prima di essa, difatti, la partecipazione elettorale era ristretta solamente a individui di sesso maschile che incontrassero determinati requisiti di censo e di reddito. Tratto da Rospi, 2021

[489] Si possono riscontrare alcune deroghe al principio di personalità come ad esempio l'articolo 56 del DPR n.361/1957 il quale prevede al co.2 che "*I ciechi, gli amputati delle mani, gli affetti da paralisi o da altro impedimento di analoga gravità esercitano il diritto elettorale con l'aiuto di un elettore della propria famiglia o, in mancanza, di un altro elettore che sia stato volontariamente scelto come accompagnatore, purché l'uno o l'altro sia iscritto in un qualsiasi Comune della Repubblica"* o nella legge n.104 del 5 febbraio 1992 all'articolo 29 viene statuito al co.3 "*Un accompagnatore di fiducia segue in cabina i cittadini handicappati impossibilitati ad esercitare autonomamente il diritto di voto. L'accompagnatore deve essere iscritto nelle liste elettorali. Nessun elettore può esercitare la funzione di accompagnatore per più di un handicappato. Sul certificato elettorale dell'accompagnatore è fatta apposita annotazione dal presidente del seggio nel quale egli ha assolto tale compito"*. È evidente che si tratti di situazioni straordinarie per le quali il legislatore ha ammesso

essere espresso dall'avente diritto tale per cui non è ammesso il cc.dd. voto per procura, ossia quella circostanza per la quale il diretto interessato delega un altro individuo affinché eserciti al suo posto il diritto al voto. Considerato all'interno del voto elettronico è necessario che l'individuo venga correttamente identificato, affinché venga garantito, anche, il principio di uguaglianza a cui corrisponde la dicitura "una testa, un voto". Tale operazione, dunque, deve avvenire attraverso adeguati sistemi di identificazione digitale come, ad esempio lo SPID o il CIE, ossia la carta d'identità elettronica. In questo frangente si può anche teorizzare l'utilizzo del CIE come sostitutivo della tessera elettorale essendo, difatti, collegata all'anagrafe senza la necessità, quindi, di dover aggiornare i registri presenti presso ogni distretto elettorale[490]. È chiaro che si pone sempre la delicata questione del digital divide[491], in quanto non tutti sono in possesso dello SPID né tantomeno del CIE. A questo problema, però, si può ribattere affermando che vi sono delle modalità alternative di identificazione dell'elettore come l'OTP, ossia l'*one time password*[492] o il caricamento della foto o scansione della carta d'identità cartacea o ancora l'autenticazione attraverso l'indirizzo e-mail. Sono tutte modalità di autenticazione conosciute e utilizzate nella vita quotidiana per poter usufruire dei più svariati servizi[493]. Per quanto riguarda il principio di uguaglianza, esso viene inteso nel senso che ogni elettore ha una sola possibilità per poter esprimere la propria preferenza alla consultazione elettorale alla quale partecipa. L'uguaglianza, quindi, può essere descritta nei termini di "*[un'] esigenza inderogabile di unicità e di irripetibilità della manifestazione di voto per ciascun elettore, relativamente alla consultazione che lo vede convocato alle urne"*[494] illustrando in maniera chiara e concisa il significato di tale principio. Al principio di uguaglianza è collegato, come già evidenziato nel corso della trattazione, il problema del cc.dd. voto multiplo. Il voto elettronico vuole proprio evitare tale situazione, la quale è più probabile che si verifichi in riferimento al voto per corrispondenza disciplinato dalla legge n.459/2001[495]. Analizzando la disciplina è chiaro che si potrebbe verificare la

una deroga al principio di personalità del voto al fine di garantire l'esercizio di tale diritto anche a chi per determinate situazioni non è in grado di esercitarlo autonomamente in virtù di quello che è il principio di uguaglianza sostanziale secondo quanto disposto dall'articolo 3 co.2 della Costituzione.

[490] Bettinelli, 2022

[491] Espressione coniata durante la presidenza Clinton negli Stati Uniti che tradotta significa divario digitale. Per divario digitale si intende, quindi, una disparità tra paesi e popolazioni nelle possibilità di accesso ai servizi telematici e alle connessioni di rete. Il divario digitale è un fenomeno ampio che ricomprende non solo il settore tecnologico, ma anche economico in quanto indica una disparità nella disponibilità economica per l'acquisto di dispositivi informatici, nonché di carattere culturale poiché indica il livello di alfabetizzazione circa l'utilizzo di tali dispositivi. Tratto da Enciclopedia Treccani, voce digital divide.

[492] Si tratta di una password valida una volta soltanto che viene generata per ogni sessione di accesso o transazione.

[493] Faccio riferimento, ad esempio, a servizi come abbonamenti online di vario genere o l'accesso all'home banking per effettuare pagamenti online, visionare la lista movimenti etc.

[494] Bettinelli, 1990

[495] Nello specifico l'art.12 della l.459/2001 disciplina il modus operandi della votazione per corrispondenza. In breve, non oltre diciotto giorni prima delle elezioni, gli uffici consolari inviano un plico agli elettori contenente il certificato elettorale, la scheda elettorale e la relativa busta ed una busta affrancata recante l'indirizzo dell'ufficio consolare competente. Al plico sono acclusi un foglio con le istruzioni circa la modalità di espressione del voto e le liste dei candidati. Se il plico non viene

circostanza per la quale un elettore dichiari di aver perso il plico precedentemente ricevuto facendo istanza per un nuovo plico per, poi, spedire entrambi alla circoscrizione Estero competente. In questo caso, è necessario tenere conto che ogni circoscrizione può scrutinare fino a tremila voti di una singola ripartizione. Il rischio, seppur minimo, di un voto multiplo è presente[496]. Il principio di uguaglianza, poi, non deve essere considerato solo nell'ottica "interna", ossia in riferimento all'elettore, ma anche da un punto di vista "esterno" di carattere strutturale, ossia nella "*predisposizione dei sistemi elettorali per la formazione […] delle assemblee rappresentative"*[497], vale a dire le condizioni fisiche per l'esercizio del diritto al voto[498] oltre al sistema prescelto, ossia maggioritario o proporzionale. In particolare la Corte costituzionale nella sentenza n.43/1961 afferma sul punto che l'uguaglianza del voto "*si concreterebbe nell'assicurare agli elettori una situazione di perfetta eguaglianza per quanto attiene all'espressione del voto, ponendo cioè ciascuno di essi nella condizione di contribuire […] alla formazione degli organi elettivi, ed escludendo, quindi, ogni possibilità di voto plurimo o voto multiplo"*[499]. La coppia personalità – uguaglianza potrebbe porre alcune criticità circa la compatibilità con la tecnologia blockchain. Non si può escludere, infatti, che in punto di personalità del voto colui che è *dietro* alla blockchain sia un soggetto diverso rispetto a colui che effettivamente si è autenticato nella rete e che vi prende parte. Si pone, dunque, la stessa problematicità in riferimento al voto elettronico in forma non presidiata, in quanto non è certo che l'individuo che si autentica nel portale adibito alla votazione elettronica sia, poi, effettivamente colui che andrà a votare. Se il principio di personalità pone qualche difficoltà circa la compatibilità con la blockchain, lo stesso lo si può affermare anche in riferimento al principio di uguaglianza. Nella rete blockchain, infatti, l'utente può effettuare un numero di *n – transazioni* per cui, se considerato il generale funzionamento di tale tecnologia, il principio di uguaglianza non verrebbe rispettato. È un problema piuttosto rilevante, poiché ciò significherebbe che un utente potrebbe votare per più volte cambiando, eventualmente, la propria idea e pertanto i risultati delle consultazioni elettorali non corrisponderebbero al vero. Difatti, in questo modo alcuni voti avrebbero un peso maggiore rispetto a chi, invece, ha optato per la scheda elettorale cartacea e la matita copiativa. È una criticità che si pone, ma è anche vero che può essere

inviato entro i diciotto giorni previsti per legge, l'elettore a quattordici giorni dalle elezioni previste può fare richiesta al capo dell'ufficio consolare, il quale può rilasciare un altro certificato elettorale munito di sigillo e una seconda scheda elettorale. Espressa la propria preferenza, l'elettore introduce nella apposita busta la/le scheda/schede elettorali, sigilla la busta, la introduce in quella affrancata assieme al tagliando staccato dal certificato elettorale che è prova dell'esercizio del diritto al voto e la spedisce non oltre il decimo giorno antecedente la data stabilita per le elezioni in Italia.

[496] Desantis, 2022

[497] Bettinelli, 1990

[498] Mi riferisco, quindi, alla preparazione dei seggi elettorali e di tutto il materiale necessario per l'esercizio del diritto al voto come la predisposizione delle schede elettorali, delle matite copiative, delle liste elettorali nonché della rimozione delle barriere architettoniche che impedirebbero a persone non deambulanti a recarsi al seggio e votare, come previsto dalla legge del 15 gennaio 1991 n.15.

[499] Sentenza n.43/1961 Corte Costituzionale.

superato questo ostacolo se si considera la particolarità del settore in cui tale tecnologia verrebbe utilizzata, pertanto sarebbe progettata effettuando una serie di scelte atte a garantire il rispetto dei principi previsti in materia elettorale. Ancora una volta, la eventuale compatibilità o meno della blockchain con i principi in materia dipende da come la rete è stata progettata. Per quanto riguarda, invece, la seconda coppia di garanzie costituzionali a tutela del diritto al voto si fa riferimento alla libertà e segretezza del voto. La libertà di voto consiste nel fatto che l'elettore deve essere in grado di esprimere in modo del tutto genuino la sua preferenza. A tal proposito, la libertà di voto non riguarda solamente l'assenza di coercizioni esterne, manipolazioni tali per cui l'elettore non sia più in grado di esprimere in modo genuino la propria preferenza, ma è anche considerata da un punto di vista "esterno", se si può dire, da parte dei candidati stessi. Si fa riferimento al cc.dd. silenzio elettorale disciplinato dalla legge del 4 aprile 1956 n.212. In particolare, all'articolo 9 è prescritto che nei giorni precedenti e in quelli stabili per l'elezione sono vietati una serie di eventi quali comizi, riunioni di propaganda e affissioni di nuovi manifesti, oltre a vietare categoricamente al giorno delle votazioni ogni forma di propaganda elettorale entro il raggio di 200 metri dall'ingresso dei seggi[500]. Si tratta di misura a presidio dell'elettore stesso il quale deve essere messo nelle condizioni di poter sviluppare una propria intelligenza politica e poter formare la propria volontà elettorale in maniera del tutto spontanea. Per garantire questo, quindi, è necessario che tutte le attività di propaganda elettorale vengano sospese durante il periodo delle elezioni al fine di evitare eventuali condizionamenti. La segretezza, invece, è la condizione per la quale il voto non deve essere palese e dunque i terzi non devono venire a conoscenza per quale partito e/o candidato si è votato. È chiaro come la segretezza del voto sia un principio rispettato dal punto di vista formale, ma non sostanziale. Dal punto di vista formale perché, se considerata la modalità tradizionale di votazione, l'elettore inserisce la scheda elettorale piegata in modo che non si vedano i simboli dei partiti all'interno dell'urna, ma dal punto di vista sostanziale è possibile che la propria preferenza venga rivelata a parenti e amici. La segretezza, inoltre, può essere considerata sia sotto un profilo interno, come "*requisito a tutela della libertà e riservatezza di ciascun votante"* sia come una garanzia esterna di carattere oggettivo attraverso la quale viene misurata la "*legittimità di ogni votazione"*[501]. Dubbi sulla compatibilità tra blockchain e articolo 48 della Costituzione, dunque, si pongono non tanto per la segretezza del voto ma, piuttosto, per la libertà di esso. La segretezza del voto, infatti, è l'aspetto che la blockchain tutela maggiormente, poiché grazie alle tecniche di crittografia, in primis l'utilizzo delle stringhe di hash, risulta arduo risalire alla preferenza espressa dall'elettore, come più volte affermato nel corso del presente lavoro. L'utilizzo di

[500] Articolo 9 co.1 e co.2 legge 4 aprile 1956 n.212.
[501] Bettinelli, 2022

varie tecniche di crittografia sono essenziali affinché possa essere garantita la segretezza del voto. Difatti, si è nella fase della consultazione elettorale nella quale vi è stata l'espressione della preferenza da parte dell'elettore per procedere poi al criptaggio del suffragio nel momento in cui avviene la transazione. La catena, quindi, funge, per così dire, da urna elettronica. Anziché inserire la scheda elettorale all'interno dell'urna fisica, il voto viene inserito all'interno di un blocco di una catena con un proprio identificativo unico e univoco al quale corrisponde l'identità dell'elettore, ma senza che ad essa vi si possa risalire. La segretezza, dunque, è garantita. In punto di libertà del voto, invece, non si può escludere il fatto che l'elettore venga coartato nell'effettuare una determinata scelta anziché un'altra. Si potrebbe, però, ribadire che questo profilo non è attinente al funzionamento della blockchain nel voto elettronico, ma è strettamente collegato alla modalità di espressione del suffragio in modalità elettronica, ossia in forma presidiata o non presidiata. È una questione che, quindi, non trova spazio circa la compatibilità o meno con l'articolo 48 della Costituzione. Questi conflitti nel concreto non vengono effettivamente considerati dal Legislatore, in quanto vi sono state varie proposte di sperimentazione del voto elettronico in Italia e in particolare nella XVIII legislatura con il disegno legge n.1323[502] si è addirittura prospettata l'introduzione di un sistema di voto che sfrutti la tecnologia blockchain. Il disegno legge in questione, però, si limita ad effettuare tale proposta solo in riferimento al voto per corrispondenza disciplinato dalla legge del 27 dicembre 2001 n.459 per i cittadini italiani residenti all'Estero. È un tentativo, seppur minimo, di introduzione nel nostro ordinamento di modernizzazione del voto e delle modalità con cui esso può essere espresso ma è altrettanto lapalissiano come sia stata una proposta di legge *monca*, in quanto non solo non è ad ampio spettro comprendendo anche i cittadini italiani residenti nel suolo nazionale, ma anche si limita a fare un riferimento alla blockchain senza ulteriori approfondimenti. Difatti, viene presa in considerazione la possibilità per la quale tale sistema non sia di possibile utilizzazione e pertanto si invita ad *"introdurre un sistema di voto da remoto per permettere all'elettore di esprimere il voto tramite una qualsiasi macchina connessa alla rete, previa identificazione e autenticazione"*[503] ferma la eventualità per la quale la blockchain non sarebbe attuabile, in questo caso deve essere vagliata la possibilità di introdurre un sistema di votazione da remoto "*per consentire all'elettore di esprimere la sua preferenza […] tramite una qualsiasi macchina connessa alla rete, previa identificazione e autenticazione"*[504]. È chiaro come il Legislatore italiano abbia cercato di introdurre almeno per il voto per corrispondenza un'alternativa rappresentata dal voto elettronico come ammodernamento del sistema finora utilizzato,

[502] Consultabile https://www.senato.it/japp/bgt/showdoc/18/DDLPRES/0/1114477/index.html?part=ddlpres_ddlpres1-articolato_articolato1
[503] Articolo 12 co.1 lettera e) disegno di legge n.1323 XVIII Legislatura.
[504] Articolo 12 co.1 lettera f) disegno di legge n.1323 XVIII Legislatura.

senza però, poi, dare seguito a tale disegno di legge. Traendo, quindi, le conclusioni si può asserire come da un punto di vista sovranazionale non si porrebbero particolari problemi di coordinamento tra blockchain e diritto al voto, in quanto i principi di personalità, uguaglianza, libertà e segretezza sembrano essere più flessibili e quindi maggiormente adattabili ad un'eventuale implementazione della blockchain nel voto elettronico. È da osservare, poi, che i principi espressi in materia a livello europeo dalle due Raccomandazioni del Consiglio d'Europa del 2004 e del 2017 abbiano dei significati simili, ma diversi rispetto ai principi previsti dall'articolo 48 della Costituzione. Sotto il profilo interno, difatti, si è riscontrata qualche difficoltà di applicazione della tecnologia blockchain al voto elettronico in punto di uguaglianza e libertà del voto. Queste riflessioni portano, quindi, ad interrogarsi se sia necessaria prospettare una modifica dell'articolo 48 della Costituzione. Difficile dare una risposta a questo quesito. Da un lato, infatti, i principi di personalità, uguaglianza, libertà e segretezza sono a presidio del diritto al voto e a tutela dell'elettore stesso, pertanto sono irrinunciabili. Dall'altro lato bisognerebbe, forse, ripensare non tanto alla loro riformulazione, ma al significato che tali principi assumono per poter aprire nuove frontiere al voto elettronico e all'utilizzo di nuove tecnologie che potrebbero incentivare l'elettorato passivo a prendere parte alle consultazioni elettorali. Il tutto si riduce ad un bilanciamento di valori tra tradizione e innovazione.

2.3. Esempi di piattaforme di voto elettronico che utilizzano la tecnologia blockchain

È appurato che il voto è un settore, tra i tanti, in cui la blockchain può trovare applicazione. In letteratura vi sono svariate proposte di sistemi di votazione elettronica basati su blockchain. Nel presente paragrafo verrà illustrato il funzionamento di alcuni dei sistemi di votazione elettronica più diffusi e conosciuti nel settore. Nonostante la presenza di un fervente interesse per questa tematica[505], vi è da considerare che il voto elettronico che sfrutta la tecnologia blockchain è solo una delle possibili soluzioni per incentivare la partecipazione elettorale, ma ciò non è sufficiente a contrastare il malessere patologico in cui versa la democrazia rappresentativa. Il tema è piuttosto recente, difatti già a partire dal 2015, pochi anni dopo la teorizzazione della blockchain e del Bitcoin[506], uno dei primi sistemi di votazione su blockchain è quello progettato da Agorà, un'impresa svizzera che si occupa di sviluppare le tecnologie da applicare ai sistemi di votazione. Nel white – paper[507] è descritto in termini analitici in che cosa consiste la tecnologica blockchain sviluppata ponendo particolare attenzione al fatto che si

[505] Ad esempio tra le piattaforme più conosciute vi sono FollowMyVote e Voataz. Per ulteriori informazioni si consulti https://followmyvote.com/blockchain-voting-the-end-to-end-process/; https://voatz.com/security-and-technology/.
[506] Ad opera di Satoshi Nakamoto nel 2008 nel celebre white – paper "*Bitcoin: A Peer – to – Peer Electronic Cash System"*.
[507] Consultabile presso https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf

tratti di una soluzione non statica, ma dinamica in quanto altamente personalizzabile. L'obiettivo di Agorà è quello di garantire un sistema di votazione che rispetti i valori democratici e che presenti le caratteristiche della (i) trasparenza, (ii) privacy, (iii) integrità, (iv) convenienza economica e (v) accessibilità[508]. Per quanto riguarda il funzionamento, Agorà presenta una sistema alquanto complesso composto da una pluralità di elementi, difatti il sistema viene definito come *"a multi-layer architecture that is based on blockchain technology"*[509], ossia una architettura multistrato basata sulla tecnologia blockchain. In totale gli strati sono cinque, ognuno dei quali comunica l'un con l'altro nelle varie fasi del procedimento elettorale. Nel dettaglio si considerano i tre elementi portanti della piattaforma, ossia (i) Skipchain, (ii) Cotena e (iii) Valeda. Per quanto riguarda Skipchain è la tecnologia alla base del *Bulletin board blockchain,* ossia una blockchain appartenente alla categoria *permissioned* costituita dai nodi approvati da Agorà e riconosciuti da terze parti come testimoni, ossia i cc.dd. *consensus nodes.* È il cuore pulsante del sistema, in quanto è il canale di comunicazione principale con gli altri strati dell'apparato e contiene tutti i dati relativi all'intero procedimento elettorale. Skipchain è un sistema innovativo, in quanto costituita da stringhe di hash che consentono di *skippare,* ossia di saltare da un blocco all'altro, in quanto sono presenti delle stringhe che afferiscono ai blocchi precedenti e delle stringhe di hash che consentono di fare riferimento ai blocchi successivi. L'innovazione consta in questo, ossia nella possibilità di navigare da un blocco all'altro della catena. Il secondo elemento portante di Agorà è Cotena, che costituisce il secondo strato consistente in una raccolta delle istantanee del *Bulletin board* nel corso del tempo. In Cotena avvengono le transazioni, per cui i *consensus nodes* approvano ogni estensione della rete. Infine vi è la rete Valeda consistente in una rete decentralizzata globale costituita da nodi il cui grado di fiducia tra loro è nullo e il cui compito consiste nel convalidare i risultati nel *Bullettin board.* Si evince da questa breve panoramica come il sistema di Agorà non sia affatto semplice, ma sia un insieme di più elementi che consentirebbero di raggiungere, o quanto meno, rispettare i principi enunciati nel white – paper. Per quanto concerne, invece, il procedimento di voto esso è composto da sei passaggi, ossia (i) configurazione, (ii) raccolta dei voti, (iii) anonimizzazione,

[508] Per quanto riguarda la *mission* di Agorà, in punto di trasparenza si fa riferimento al principio di verificabilità tale per cui ogni cittadino ha il diritto di verificare se il suo voto è stato correttamente registrato e se è stato manipolato. In punto di privacy, Agorà fa riferimento ai sistemi di crittografazione elaborati per garantire l'anonimato tale per cui non è possibile risalire alle preferenze espresse dall'elettore. Il sistema di votazione, inoltre deve garantire l'integrità, ossia solo chi può esercitare il diritto al voto è autorizzato ad effettuare tale operazione. Si guarda, poi, anche al lato economico. Difatti la piattaforma di votazione deve assicurare un risparmio di spesa per coloro che decidono di implementare Agorà. Infine, la soluzione proposta deve essere in grado di funzionare non solo sui supporti informatici governativi, ma anche personali come computers e smartphone. L'obiettivo è quello di creare un sistema di voto non presidiato, in cui gli elettori possono comodamente votare da qualsiasi device e in qualsiasi momento. È interessante osservare che nella maggior parte dei casi i sistemi di votazione elettronica sono di carattere presidiato, ossia richiedono la presenza di una pubblica autorità, ma l'obiettivo a lungo termine è quello di creare dei sistemi di votazione elettronica non presidiati nel rispetto dei principi espressi in materia di voto con particolare riferimento alla libertà e segretezza del voto.

[509] https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf

(iv) decriptazione, (v) conteggio e (vi) auditing. La prima fase è di carattere preparatorio consistente nella configurazione del sistema. In questa fase, difatti, viene predisposto l'intero assetto della consultazione elettorale. Viene creato un *configuration file* nel quale viene inserito un insieme di elementi, come la lista degli elettori, dei candidati, il tipo di elezione e la sua durata. Una volta creato questo file, i pubblici ufficiali generano un ID che rappresenta l'evento elettorale attraverso una funzione di hash e firmano il file creato, il quale ha valenza di prova del fatto che sono gli organizzatori dell'evento. Vi è poi la raccolta dei voti, per cui gli elettori esprimono le loro preferenze. La particolarità di Agorà consiste nel fatto che consente di votare nella forma non presidiata, ma anche in quella presidiata, per cui all'elettore viene dato un ampio margine di scelta sul modo con cui esprimere il proprio suffragio. È un sistema progettato in modo *smart* che consente di sfruttare tutti i vantaggi forniti dal voto elettronico. Una volta espresso il voto, esso viene crittografato utilizzando un software apposito[510]. Affinché vi sia una corrispondenza tra il voto espresso e il voto crittografato, Agorà utilizza come sistema di verifica il *Cast – or – Challenge Validation*[511]. Il terzo step consiste nell'anonimizzazione, affinché venga assicurata la privacy degli elettori. L'obiettivo è quello di far sì che al voto espresso non sia possibile risalire all'elettore nel momento in cui vengono decrittati durante la fase del conteggio. Vi è poi la fase della decrittazione affinché si possa passare al conteggio dei voti[512]. L'ultimo step è l'auditing, ossia la possibilità di verificare la correttezza dell'intera procedura elettorale. In questo frangente, entrano in gioco i *Citizen Auditor Nodes,* ossia nodi specificamente preposti a tale operazione, i quali possono essere gli organizzatori dell'evento, gli elettori o terze parti. Se la procedura ha un esito positivo, allora vi è una attestazione finale che viene firmata digitalmente con la chiave privata di colui che ha effettuato tale operazione. Simile ad Agorà è il sistema ideato da Kaspersky Innovation Lab nel 2020, ossia Polys[513]. L'obiettivo di Polys è quello di fornire un servizio di votazione elettronica che consenta una verificabilità in ogni fase di votazione. Alla base vi è una piattaforma blockchain, ossia Exonum, appartenente alla tipologia di blockchain permissioned. Oltre

[510] Nel white – paper non è specificato a quale software si riferisce. Viene specificato che si tratta di una crittografazione che avviene anche con l'ausilio di una chiave pubblica nei *consensus nodes* della rete Agorà.

[511] Sistema ideato da Josh Benaloh nel 2006 che affronta il problema della possibile discrepanza tra quanto espresso dall'elettore e il voto crittografato. L'idea alla base è piuttosto semplice, ossia si tratta di utilizzare una *interactive proof* per la quale un *prover* può essere sfidato, ossia *challenged,* n-volte da un *verifier* a rispondere a certe domande a cui è possibile dare risposta solo se determinate affermazioni sono vere. Nel concreto si traduce nella circostanza per la quale vi è un soggetto che afferma di avere una chiave di decrittazione che corrisponde a una chiave di crittografia. Il *verifier* può selezionare determinati valori, crittografarli con la chiave pubblica e sfidare il *prover* a decriptarla. Se l'operazione si conclude con successo, allora il *verifier* si convince che il *prover* effettivamente detiene al chiave di decrittazione. Per approfondire si veda Josh Benaloh, "*Simple Verifiable Elections",* June 14th 2006 reperibile su https://home.ipipan.waw.pl/w.jamroga/papers/benalohGT23evote-final-arxiv.pdf

[512] In questa fase i nodi di Cothority procedono alla decrittazione delle schede elettorali per poi pubblicare su *Bulletin Board* i voti cos' decrittati. Cothority è un elemento di Cotena, ossia il secondo strato di Agorà e gestisce un registro aggiuntivo che formato da una serie di transazioni Bitcoin selezionate.

[513] Per ulteriori dettagli si veda il white – paper "*Polys online voting system"* di Kaspersky. Per ulteriori informazioni si veda https://gsma.my.site.com/mwcoem/servlet/servlet.FileDownload?file=00P690000308eNaEAI

a Exonum vi è un *service layer*[514] e il *polys – protocol library.* L'elemento più interessante è la piattaforma blockchain utilizzata. Exonum è una rete blockchain dotata di un linguaggio di programmazione proprio che consente di effettuare un numero elevato di transazioni fronteggiando il problema della scalabilità grazie all'utilizzo degli *smart contracts,* i quali vengono utilizzati dai *gatekeepers* della rete solo quando vi è stato il raggiungimento del consenso. A tal proposito, nel white – paper non viene specificato quale sia l'algoritmo di consenso che viene utilizzato nella rete, ma è chiaro che non è né il Proof – of – Work né il Proof – of – Stake, in quanto è espressamente dichiarato che per il raggiungimento del consenso Exonum "*does not require mining or economic rewards"*[515]. Per quanto attiene al processo di votazione, esso si suddivide per gradi. Come in ogni consultazione elettorale vi è la fase preparatoria. Polys prevede un primo *set – up* in cui le pubbliche autorità ottengono le loro chiavi per la firma elettronica dei messaggi. Tali chiavi pubbliche vengono, poi, aggiunte ai nodi di convalida della blockchain ai fini della transazione. Una volta che la rete è configurata viene messa in atto la configurazione del servizio. In particolare, Polys non prevede un sistema di identificazione interno ma l'utilizzo di metodi di identificazione esterni. Sempre nella fase di configurazione, viene creata una *access control list,* ossia una lista di controllo degli accessi contenente diversi parametri[516]. A seconda della modalità di identificazione dell'elettore, l'organizzatore dell'evento prepara la ACL[517] ed effettua una richiesta al *service layer.* L'ACL assegna a ciascun elettore un identificativo interno e immagazzina il link all'ID esterno nel database del *service.* Per quanto riguarda, invece, il voto, l'organizzatore specifica una serie di parametri[518]oltre a indicare il come parteciperà l'elettore all'elezione, la tipologia di ballottaggio e il metodo di conteggio. La particolarità di Polys consiste non solo nella sua architettura, ma anche nel fatto che presta attenzione alla tipologia di elezione in cui tale sistema intende essere utilizzato, poiché distingue a seconda che si tratti di una elezione con una sola scelta come, ad esempio, un referendum, a scelta multipla come le elezioni amministrative locali e nazionali o cumulative, ossia una modalità particolare in cui

[514] È responsabile dell'autenticazione degli utenti, nonché per la firma di messaggi detti *blinded* e per il compimento di operazioni di sistema come l'invio di notifiche. Il *polys – protocol library* è uno strato ulteriore del sistema e consente di effettuare operazioni con entità di alto livello.

[515] Il che vuol dire che Exonum non richiede alcuna operazione di mining né di accantonamento di fondi, tipici del Proof – of – Work e del Proof – of – Stake. Ricordando in breve in che cosa consistono questi due protocolli di consenso, il PoW presenta dei nodi specializzati, ossia *miners* il cui compito è quello di risolvere complessi puzzle matematici forniti dall'algoritmo di consenso. Una volta risolto il problema matematico, è possibile un nuovo blocco alla catena qualora il valore trovato dal minatore sia corrispondente al valore di riferimento o se è inferiore ad esso. Il PoS è un algoritmo di consenso in cui ogni nodo della rete accantona un certo ammontare di monete detto, appunto, *stake*. In base all'ammontare accantonato, i nodi possono essere selezionati per la creazione di nuovi blocchi all'interno della catena. In questo caso, dunque, ciò che conta non è il lavoro svolto, ma il patrimonio a disposizione dei nodi.

[516] Tra cui si ricorda (i) la modalità di autenticazione dell'elettore, (ii) se i voti espressi hanno tutti lo stesso "peso", (iii) se la lista degli elettori è predefinita o se essi possono aggiungersi successivamente.

[517] Acronimo per access control list.

[518] Ossia (i) l'identità dell'elettore tratta dall'ACL, (ii) la descrizione della operazione elettorale, (iii) la lista delle opzione tra cui scegliere e (iv) la durata della consultazione.

l'elettore deve distribuire il suo suffragio tra una serie di opzioni disponibili[519]. Ulteriore passaggio è l'autenticazione dell'elettore, la quale avviene attraverso l'utilizzo di un servizio esterno. L'utente effettua una richiesta al servizio usufruito affermando che possiede un account esterno, per esempio attraverso l'indirizzo e-mail o il numero di cellullare. Una volta confermato questo account esterno, il servizio di autenticazione crea un ID interno generando un *random secret* il cui valore di hash viene inviato alla blockchain. Successivamente lo *smart contract* verifica se il *secret* e il valore di hash sono coincidenti. Lo step successivo è l'ottenimento della scheda elettorale da parte dell'elettore autenticato attraverso una *blind signature.* In breve, l'elettore crea un paio di chiavi random non collegate al proprio account che viene utilizzato per firmare la transazione e la scheda elettorale. Il valore di hash della chiave pubblica serve come token di autorizzazione. Questi due elementi sono essenziali, in quando consentono di verificare se la persona che ha utilizzato il token è la stessa che detiene la coppia di chiavi per la firma della transazione. Infine, vi è la fase del conteggio in cui i valori criptati vengono sommati a quelli già presenti sulla rete. Come Agorà, anche Polys è una soluzione che può essere utilizzata sia nel voto elettronico presidiato tramite appositi macchinari sia nel voto elettronico non presidiato accedendo alla piattaforma predisposta. È necessario essere dotati di un device elettronico, quale uno smartphone, computer o tablet e di una buona connessione Internet. Si può affermare, a seguito di questa breve panoramica, come vi siano delle proposte interessanti in materia le quali condividono la suddivisione in fasi della consultazione elettorale con a capo sempre l'inizializzazione della procedura e l'autenticazione degli elettori. Inoltre, ulteriore elemento di collegamento è la presenza di più elementi a contorno della blockchain che consentono il funzionamento dell'intero apparato al fine di rispettare gli standard minimi, quali sicurezza e verificabilità. Il loro funzionamento non è semplice, ma non bisogna temere che si tratti di operazioni lunghe e laboriose, in quanto il tutto si verifica in un *click* all'insaputa, per così dire, dell'elettore il quale è inconscio dei meccanismi che si mettono in moto nel momento in cui esprime il proprio suffragio. Nel prossimo paragrafo verranno illustrati alcune opportunità che la tecnologia blockchain apporta nel voto elettronico.

[519] Per approfondire questo aspetto si veda il white – paper.

3. Opportunità dell'utilizzo delle blockchain nel voto elettronico

Dopo aver studiato il funzionamento della tecnologia blockchain applicata al voto elettronico, anche attraverso alcuni esempi concreti, e constatate alcune difficoltà applicative per quanto riguarda il rispetto dei principi fondamentali espressi in materia elettorale, non resta che esaminare alcuni dei vantaggi forniti dall'utilizzo di tale tecnologia nel settore elettorale. È indubbio che tale tecnologica offra numerosi vantaggi, ma ai fini della trattazione vengono considerati la velocità nello spoglio e le caratteristiche della trasparenza, sicurezza e immutabilità in quanto maggiormente aderenti al voto elettronico.

3.1. Velocità nello spoglio elettorale

Una delle fasi più delicate di tutta la consultazione elettorale è il conteggio dei voti, in quanto va a determinare coloro che saranno i rappresentanti in Parlamento e che influenzeranno la politica del Paese per il prossimo mandato. Lo scrutinio dei voti è disciplinato nel nostro ordinamento dal DPR n.361/1957 al Titolo V, il quale a partire dall'articolo 67 descrive come avviene il conteggio. Osservando il Titolo V si può affermare come la fase dello scrutinio sia suddivisa in due momenti, da un lato il conteggio che avviene all'interno del seggio ad opera del presidente, del segretario e degli scrutatori e dall'altro la verifica e la suddivisione in seggi ad opera dell'Ufficio centrale nazionale secondo quanto previsto dall'articolo 83[520]. Ai fini della trattazione non verrà descritto l'iter effettuato dall'Ufficio centrale nazionale, poiché si tratta di un procedimento lungo e complesso, ma si considererà solo quanto avviene all'interno del seggio. Si considera questo aspetto sia per ragioni di lunghezza della trattazione, la quale altrimenti sarebbe assai tediosa, sia perché si tratta di una fase che avviene immediatamente dopo la chiusura delle votazioni e che funge da base per i conteggi e le verifiche successivamente effettuate. L'articolo 67 del DPR n.361/1957 prevede una prima fase di inizializzazione nella quale il presidente del seggio dichiara chiusa la votazione e accerta il numero dei votanti risultanti dalle liste elettorali[521]. Tali liste devono essere firmate in ogni foglio da due scrutatori e dal presidente per poi essere inserite in un plico sigillato firmato dal presidente e da almeno due scrutatori. Il plico può essere firmato anche dai rappresentati delle liste dei candidati se lo desiderano.

[520] Non è possibile riportare per intero il testo dell'articolo 83 del DPR 361/1957, poiché eccessivamente lungo, ma è possibile comunque affermare come il suo compito consiste nel determinare la cifra elettorale nazionale di ogni lista, la quale è determinata dalla somma di tutte le cifre elettorali circoscrizionali di ogni circoscrizione, nonché stabilire la cifra nazionale elettorale di ciascuna coalizione di liste collegate data dalla somma delle cifre elettorali nazionali di tutte le liste che compongono la coalizione e dalla cifra elettorale nazionale delle liste non collegate. Successivamente individua la coalizione di liste o la lista non collegata che ha ottenuto il maggior numero di voti. Al punto n.3) del co.1 dell'art.83 viene, poi, descritto il procedimento di individuazione delle coalizioni dl liste secondo le soglie previste ex lege per poi procedere nei commi successivi al riparto dei seggi.

[521] Vengono considerate anche coloro che sono appartenenti alle Forze Armate e al Corpo nazionale dei vigili del fuoco, nonché dei naviganti fuori residenza per motivi di imbarco e dei soggetti degenti nelle strutture ospedaliere.

È chiaro che durante la consultazione non tutti gli iscritti alle liste elettorali si presenteranno alle urne, pertanto, ai sensi del comma 3 dell'articolo 67 il presidente del seggio estrae e conta le schede rimaste nella cassetta e verifica se il numero delle schede rimaste corrisponda al numero degli elettori iscritti alle liste, ma che non hanno votato. Successivamente, secondo quanto previsto dall'articolo 68 del DPR n.361/1957 si procede allo spoglio delle schede. Uno scrutatore estratto a sorte preleva ciascuna scheda dall'urna e la consegna al presidente, il quale enuncia ad alta voce il contrassegno della lista alla quale è stato attribuito il voto. La scheda passa, poi, ad un altro scrutatore che assieme al segretario prende nota dei voti di ciascuna lista. Infine, il segretario proclama ad alta voce i voti di lista e un terzo scrutatore ripone le schede spogliate nella cassetta dalla quale sono state tolte le schede inutilizzate. Si comprende come sia una fase molto delicata, in cui è necessario che vi sia un perfetto coordinamento tra presidente del seggio, segretario e scrutatori affinché il conteggio[522] dei voti avvenga secondo le modalità prescritte. Lo scrutinio prosegue con la pronuncia da parte del presidente del seggio delle difficoltà e degli eventuali incidenti che si sono verificati nelle varie operazioni e decide provvisoriamente sull'assegnazione o meno dei voti contestati[523]. Una volta concluso lo scrutinio, il presidente procede alla formazione, ex art.72 DPR n.361/1957, di vari plichi[524]. Le operazioni così descritte devono essere effettuate entro un determinato arco temporale prescritto dall'art.73, ossia "*subito dopo la chiusura della votazione proseguite senza interruzione ed ultimate entro le ore 14 del giorno seguente"*[525]. Tutte le operazioni così effettuate devono essere messe a verbale, il quale è redatto dal segretario in doppia copia. Successivamente il presidente dichiara il risultato dello scrutinio e lo fa mettere a verbale, per poi, inviare il plico[526] chiuso e sigillato alla Cancelleria del Tribunale nella cui circoscrizione ha sede la sezione, la quale provvederà all'invio del materiale così ricevuto alla Cancelleria della Corte d'Appello o del Tribunale del capoluogo della circoscrizione. La seconda copia del verbale viene depositata presso la Segreteria del Comune affinché ogni elettore possa prenderne

[522] Sul punto, qualora vi dovessero essere dei dubbi interpretativi l'articolo 69 giunge in soccorso statuendo "*La validità dei voti contenuti nella scheda deve essere ammessa ogni qualvolta possa desumersi la volontà effettiva dell'elettore […]. Quando un unico segno sia stato traccia su più rettangoli, il voto di intende riferito al contrassegno su cui insiste la parte prevalente del segno stesso".* L'articolo 70, invece, indica quando il voto è nullo, ossia "*[…] sono nulli i voti contenuti in schede che presentino scritture o segni tali da far ritenere, in modo inoppugnabile, che l'elettore abbia voluto far riconoscere il proprio voto. Sono, altresì, nulli i voti contenuti in schede che non siano quelle prescritte dagll'art.31, o che non portino la firma o il bollo richiesti dagli artt.45 e 46".* L'articolo 31 descrive l'impostazione delle schede elettorali, mentre gli artt.45 e 46 prevedono il bollo della sezione afferente al plico che contiene le schede elettorali.

[523] Art.71 DPR n.361/1957.

[524] Ex art.72 co.1 e co.3 DPR n.361/1957 i plichi che il presidente del seggio deve procedere a formare contengono (i) le schede corrispondenti ai voti contestati, (ii) le schede corrispondenti a voti nulli, (iii) le schede deteriorate e le schede consegnate senza appendice o numero o bollo o firma dello scrutatore e (iv) le schede corrispondenti a voti validi ed una copia delle tabelle di scrutinio. Tali plichi, poi, devono recare l'indicazione della sezione, il sigillo col bollo dell'Ufficio, le firme dei rappresentanti di lista, del presidente e di almeno due scrutatori.

[525] Articolo 73 co.1 DPR n.361/1957.

[526] Contenente il verbale con le schede e tutti i plichi e i documenti previsti dal co.3 dell'art.72.

visione, se lo desidera[527]. Il fatto che gli elettori possano prendere visione del verbale è in ossequio al principio di verificabilità e trasparenza, in quanto è possibile verificare la presenza di eventuali errori nel conteggio o nelle operazioni di scrutinio. È, quindi, un rendere conto agli elettori delle operazioni che sono state effettuate. Da questa disamina è evidente che si tratta di operazioni lunghe e complesse nelle quali si insinua l'errore umano. Nel momento in cui dovesse esserci un errore in una di queste operazioni l'intero procedimento dovrebbe essere effettuato nuovamente con ulteriore dispendio di tempo ed energie. La difficoltà dello scrutinio non riguarda solamente il dover rispettare ogni singola fase prevista e il ruolo di ogni soggetto del seggio, ma anche nel come interpretare i segni apposti alle schede elettorali, nonché verificarne la corretta compilazione[528]. Ulteriore elemento da considerare poi è la durata dell'operazione di spoglio come previsto dall'art.73 del DPR n.361/1957. È evidente come si tratti di una procedura lunga e laboriosa che mette a dura prova coloro che la devono effettuare sia dal punto di vista fisico sia dal punto di vista mentale, pertanto il rischio di commettere qualche errore è presente. La tecnologia blockchain interviene su questo punto, in quanto consente di effettuare uno spoglio dei voti più celere. Nelle varie proposte di sistemi di votazione elettronica che utilizzano la tecnologia blockchain viene considerato anche l'aspetto del conteggio tra le varie fasi della consultazione elettorale. Sul punto vi è da fare una considerazione. Qualora si volesse implementare tale tecnologia, nel nostro ordinamento, nei sistemi di votazione elettronica oltre a doversi scontrare con alcuni problemi di compatibilità a livello costituzionale, il Legislatore dovrebbe provvedere ad una modifica del Titolo V del DPR n.361/1957 e dedicare una parte allo scrutinio in via digitale oppure vi dovrebbe essere l'introduzione di un nuovo testo normativo in materia, al fine di ammettere l'utilizzo di soluzioni tecnologie per lo scrutinio dei voti. Ciò che interessa è comprendere come avviene il conteggio, ossia il cc.dd. *tallying,* nella blockchain. In letteratura gran parte delle proposte di *tallying* partono dallo stesso presupposto, ossia garantire un sistema di votazione elettronica che sia trasparente e che consenta la verificabilità del voto. In questo contesto più che parlare di conteggio vero e proprio si parla di *self-tallying.* Essa è una proprietà della rete blockchain strettamente correlata alla caratteristica della verificabilità per cui ogni elettore o qualsiasi parte terza può effettuare un conteggio dei voti una volta che tutte le preferenze sono state registrate[529]. Grazie a questa proprietà si sfrutta un ulteriore caratteristica della blockchain, ossia la decentralizzazione tale per cui non è necessaria un'autorità terza che effettui tale operazione. Si coglie, quindi, fin da subito la differenza rispetto al

[527] Art.75 DPR n.361/1957.
[528] Per esempio, il sistema vigente prevede che il voto si esprime tracciando un segno sul contrassegno della lista scelta. Se espresso così, il voto è valido sia per la lista sia per il candidato uninominale a essa collegato. La seconda opzione di voto prevede un segno sul nome del candidato uninominale il voto è espresso anche per la lista ad esso collegata. Se ci sono più liste collegate, il voto è ripartito tra le liste di coalizione. Per ulteriori informazioni https://www.interno.gov.it/it/notizie/quando-e-come-vota-elezionipolitiche2022
[529] McCorry , Shahandashti , & Hao, 2017

sistema tradizionale il quale, invece, prevede il coinvolgimento di più soggetti[530] ossia il presidente del seggio, il segretario e gli scrutatori. È una proprietà, inoltre, che garantisce la segretezza assoluta della scheda elettorale, in quanto affinché la procedura di conteggio possa avere inizio è necessario che tutti abbiano votato e consente a terze parti di verificare che gli elettori abbiano correttamente seguito il protocollo di votazione previsto dalla rete blockchain[531]. Nelle proposte che si sono vagliate[532] vengono descritte minuziosamente le singole componenti del sistema proposto, nonché il complesso funzionamento del protocollo del *self-tallying* condividendo l'obiettivo di garantire un sistema di votazione che sia sicuro e privo di brogli elettorali. Gli studi in materia hanno evidenziato come vi sia un problema di *fairness*, ossia di correttezza, in quanto l'ultimo elettore può calcolare il conteggio prima di chiunque altro[533] essendo, per così dire, l'ultimo della catena. Il problema della *fairness* si traduce, quindi, in una questione di adattamento e di abolizione dell'intera procedura. Per quanto attiene al primo problema, essere a conoscenza del conteggio fa sì che questo possa influenzare l'ultimo elettore nel manifestare il proprio suffragio. Per quanto concerne, invece, il secondo problema si pone il rischio che l'elettore non essendo soddisfatto dell'andamento della consultazione decida di non votare compromettendo, quindi, l'intera operazione[534]. Per fronteggiare queste criticità il sistema proposto da Lu et al grazie al *time – limited ballot secrecy* consente di superare la questione della correttezza e le problematicità ad essa annessa. In particolare, il *time – limited ballot secrecy* è un requisito del sistema progettato, il quale prevede che per un determinato ammontare di tempo il contenuto di ogni scheda elettorale rimane segreto e una parte del conteggio effettuato rimane riservato[535]. Questo avviene grazie al *time – lock puzzle,* un algoritmo che genera un puzzle la cui soluzione rimane segreta per un certo periodo di tempo, pertanto il puzzle non può essere risolto fino allo scadere del tempo previsto[536]. In generale si può affermare come l'aspetto del conteggio del voto non sia particolarmente approfondito nelle varie proposte di *e-voting* su blockchain[537] nonostante sia una delle fasi più importanti e delicate dell'intera consultazione elettorale. Malgrado ciò, è chiaro come l'ausilio di tale tecnologia consenta un conteggio più celere e privo di errori a differenza della modalità tradizionale, la quale prevede il coinvolgimento di una pluralità di soggetti. Inoltre, con la blockchain verrebbero risolti molti problemi di natura interpretativa circa l'apposizione del segno sulla scheda elettorale e la presenza di eventuali voti nulli. In conclusione, dunque, la tecnologia blockchain

[530] Sempre in riferimento al sistema di votazione in Italia.
[531] McCorry , Shahandashti , & Hao, 2017
[532] Si veda ad esempio Lu, et al., 2023; Stančíková & Homoliak, 2023 e Kiayias & Yung, 2002
[533] McCorry , Shahandashti , & Hao , 2017
[534] *Ibidem*
[535] Lu , et al., 2023
[536] *Ibidem*
[537] Si veda ad esempio la white – paper di Agorà a cui è dato un piccolo spazio al *tallying* a discapito di tutte le altre fasi di votazione.

potrebbe essere un valido aiuto nella fase ultima della consultazione elettorale eliminando la necessità di una pluralità di soggetti quali il presidente del seggio, il segretario e gli scrutatori e riducendo notevolmente l'errore umano. È solo una delle tante possibili utilizzazioni di tale tecnologia nel settore elettorale che consentirebbe di costruire un sistema elettorale più sicuro ed efficiente.

3.2. Trasparenza, sicurezza e immutabilità: l'ABC della tecnologia blockchain applicato al voto

Nel 2008, quando la blockchain fu teorizzata per la prima volta nel white – paper di Satoshi Nakamoto venne compreso immediatamente il potenziale di questa tecnologia soprattutto in termini di trasparenza, sicurezza e immutabilità che resero la blockchain appetibile per un settore come quello finanziario. Con il passare del tempo, ci si rese conto che grazie a queste tre caratteristiche tale tecnologia potesse essere impiegata in svariati settori, tra cui quello elettorale e in particolare essere calata nel contesto del voto elettronico. Trasparenza, sicurezza e immutabilità formano l'ABC della blockchain e che, come si vedrà, sono delle proprietà intrinsecamente correlate tra loro e che si rivelano preziose per le consultazioni elettorali. Nell'immaginario collettivo, la trasparenza è collegata alle Pubbliche Amministrazioni e si traduce nella possibilità per il cittadino di accedere a tutte le informazioni che riguardano l'organizzazione e le attività delle P.A. Si fa riferimento, a tal proposito, al diritto di accesso disciplinato dall'articolo 22 della legge sul procedimento amministrativo[538] e al diritto di accesso civico disciplinato dal D.lgs. n.33/2013[539]. Nella blockchain la trasparenza assume un significato leggermente diverso. Considerato che la rete blockchain è una DLT, ossia una *Distributed Ledger Technology,* per cui è una tecnologia a registro distribuito è chiaro che ogni transazione che avviene nella rete è tracciabile essendoci una rete estesa di nodi ognuno dei quali detiene una copia delle transazioni effettuate nel network[540]. Non essendoci un'autorità terza, come avviene per le blockchain *permissioned*[541]*,* per necessità le operazioni che sono state eseguite devono essere tracciabili. A tal proposito vi è da osservare che la trasparenza è garantita non solo dal fatto che chiunque può accedere al network e verificare le transazioni che sono avvenute, ma anche dal fatto che sono presenti alcuni siti Internet che consentono all'utente esterno di verificare in tempo reale quali transazioni sono avvenute, il mittente e il destinatario, l'orario e il blocco che è stato aggiunto alla

[538] Articolo 22 legge 7 agosto 1990 n.241.
[539] Si vedano gli artt. 5 e 5-bis del D.lgs. n.33/2013.
[540] Politou , Casino, Alepis , & Patsakis, 2019
[541] Anche nelle reti *permissioned* vi è l'elemento della trasparenza, in quanto il grado di fiducia tra i nodi è molto elevato, il che richiede che tutte le operazioni debbano essere tracciabili. Difatti, qualora vi fosse un'operazione malevola consistente in un tentativo di manomissione dei blocchi, tale è immediatamente visibile alla rete, pertanto la trasparenza è strettamente correlata con la caratteristica dell'immutabilità.

catena oltre al valore di scambio della criptovaluta che può essere l'Ether di Ethereum o il Bitcoin[542]. Trasparenza e tracciabilità, quindi, sono strettamente correlate tra loro. La tracciabilità, difatti, si riscontra nell'utilizzo del marcatore temporale, ossia del *time stamp* il quale individua la data, l'ora e il giorno in cui la transazione è stata effettuata. Calando la proprietà della trasparenza nelle procedure elettorali si può affermare che nel voto analogico essa è garantita dalle attività che vengono effettuate nel seggio. A titolo di esempio, si può far riferimento al fatto che davanti all'elettore viene dispiegata la scheda elettorale o le schede elettorali, a seconda della consultazione in atto, gli venga consegnata la matita copiativa o il semplice fatto che l'elettore, una volta espressa la propria preferenza, inserisce la scheda nell'urna davanti agli scrutatori, al presidente del seggio e al segretario. Si tratta di operazioni che avvengono, per così dire, alla luce del sole davanti a più soggetti che fungono da testimoni di quanto avvenuto. Nel voto elettronico la trasparenza può essere declinata nelle caratteristiche che un sistema di votazione elettronica deve avere e in particolare con riferimento alla verificabilità, ossia all'*audit.* L'elettore, infatti, grazie alla caratteristica della trasparenza che rende ogni operazione tracciabile è in grado di verificare personalmente se il proprio voto sia stato correttamente immesso nella catena e quindi se la transazione è andata a buon fine. La trasparenza, poi, è anche collegata alla fase finale della consultazione elettorale, ossia il conteggio. Dal momento che ogni transazione è registrata, ciò consente di verificare nell'immediato se vi sia stato qualche tentativo di manipolazione o qualche tentativo di voto multiplo. Sul punto vengono in gioco le due successive proprietà della blockchain, ossia la sicurezza e l'immutabilità intrinsecamente correlate tra loro. La sicurezza nella blockchain è garantita dall'utilizzo di sistemi di crittografia avanzata come, ad esempio, le già citate le funzioni di hash. Riprendendo brevemente in che cosa consistono, in quanto ciò consente di comprendere la proprietà dell'immutabilità e di conseguenza la sicurezza della blockchain, le funzioni di hash sono tra le tecniche di crittografia più utilizzate e nell'ambito della blockchain hanno la funzione di collegare i blocchi della catena. Il collegamento tra blocchi, infatti, avviene attraverso il richiamo dell'hash precedente nel blocco successivo. Il valore di hash viene generato a partire da un input, il quale viene trasformato in un codice alfanumerico, ossia nell'output. Generalmente, nella blockchain viene utilizzato l'algoritmo SHA-256, il quale genera un messaggio, ossia l'output della lunghezza di 64 caratteri. Ciò che interessa, però, è una delle caratteristiche delle funzioni di hash poiché essa è ciò che garantiscono la sicurezza e l'immutabilità della blockchain. Nello specifico, un dato input produce un output e da esso non è possibile risalire a ritroso al dato di partenza[543]. È, quindi, una funzione unilaterale. Traslato nella rete blockchain, la funzione di hash assicura l'immutabilità, in

[542] Si veda ad esempio https://etherscan.io/txs, e https://btcscan.org/.
[543] GENÇOĞLU1, 2022

quanto una volta completata la transazione e quindi aggiunto il blocco alla catena non è più possibile modificarlo, pertanto qualsiasi tentativo di alterazione del blocco così creato o di attacco alla rete è immediatamente visibile[544]. Ed è proprio qui che si comprendono i vantaggi della tecnologia blockchain applicata al voto elettronico. Grazie a queste caratteristiche viene rispettato il principio di uguaglianza e si evita il cc.dd. voto multiplo, in quanto una volta completata la procedura di votazione e aggiunto il blocco alla catena, non è più possibile per l'elettore votare una seconda volta, in quanto si è già registrato e autenticato all'interno del sistema. Anche nel voto in forma analogica l'elettore non può votare *n-volte*, poiché una volta identificato al seggio ciò assicura il rispetto della formula "una testa un voto". Se nel voto analogico l'immutabilità si traduce nell'impossibilità di eliminare il segno apposto sulla scheda elettorale con la matita copiativa, nel voto elettronico si traduce nell'integrità del voto, in quanto una volta espresso non può più essere modificato. Infine, tali caratteristiche tutelano la rete blockchain da eventuali attacchi esterni, anche se non si può escludere la possibilità che vi sia qualche aggressione informatica o l'utilizzazione di bug di sistema per il compimento di frodi, come nella famosa vicenda di The DAO. Nonostante la presenza di possibili attacchi informatici, tale tecnologia è ampiamente studiata nel settore elettorale in quanto se ne sono comprese le potenzialità. Grazie all'ABC rappresentato dalle caratteristiche della trasparenza, sicurezza e immutabilità è possibile sfruttare la tecnologia blockchain nel voto elettronico, in quanto vengono così garantite elezioni sicure i cui voti sono tracciabili andando, quindi, a preservare l'integrità dei risultati della consultazione elettorale. C'è, però, da considerare come nonostante la presenza di questi vantaggi renda allettante l'utilizzo di tale tecnologia nel voto elettronico, siano presenti anche delle sfide che tale settore pone che verranno analizzate nel prossimo paragrafo.

[544] Politou, Casino, Alepis, & Patsakis, 2019

4. Le sfide poste dalla blockchain nel voto elettronico

Una trattazione non sarebbe completa se, dopo aver analizzato le opportunità offerte dalla blockchain nel voto elettronico, non si studiassero anche i risvolti negativi, anzi, le sfide che tale tecnologia pone alle democrazie odierne ai fini della sua implementazione nel settore elettorale. Le due maggiori criticità che si riscontrano in riferimento a tale settore sono individuate nella carenza di standard e nel problema della scalabilità. A queste problematicità si cercherà di formulare alcune soluzioni senza avere, però, la pretesa di risolvere le criticità evidenziate.

4.1. Assenza di standard comuni

È indubbio che la tecnologia blockchain sia una delle scoperte più innovative e rivoluzionarie degli ultimi decenni, in quanto ha consentito per la prima volta di effettuare scambi di denaro, in questo caso criptovalute, in assenza di un soggetto terzo come, ad esempio, la banca o un'autorità pubblica. L'obiettivo di Nakamoto era quello di creare un sistema alternativo rispetto ai tradizionali metodi di pagamento che permettesse di superare il problema del *trust,* ossia della fiducia tra le parti[545]. Nonostante la tecnologia in questione offra molte opportunità e vantaggi nel suo impiego, è anche evidente come ponga alcune sfide nella sua utilizzazione. Tra queste emerge una assenza di standard comuni. Si potrebbe affermare che sia presente, in un certo qual senso, un modello di riferimento ossia quello teorizzato da Nakamoto nel 2008 ma è altrettanto vero che fin da subito sono emerse numerose varianti, pertanto è difficile affermare che sia presente un unico modello a cui appoggiarsi. Non è semplice fornire una corretta definizione di standard, poiché è un lemma che assume diverse sfumature di significato a seconda del contesto, ma per quanto attiene alla blockchain si può fare riferimento al linguaggio tecnico. Per standard, dunque, si intende l'insieme di regole, leggi e raccomandazioni che determinano i requisiti essenziali che un prodotto deve avere[546]. Nel settore elettorale questo insieme di regole che individuano i requisiti essenziali si traducono non in standard, ma in principi. Difatti, nella maggior parte delle proposte in letteratura circa l'utilizzo di tale tecnologia nel voto elettronico non viene fatto riferimento a standard di carattere tecnico a cui la blockchain deve sottostare, ma a principi generali a cui la piattaforma di *e-voting* deve ottemperare affinché vi possano essere delle consultazioni elettorali che siano sicure e trasparenti. Non vi è, quindi, un'aporia di principi in materia elettorale, ma di standard comuni a cui la tecnologia blockchain dovrebbe sottostare in riferimento a questo particolare settore. Difatti, dall'analisi finora condotta è emerso come la blockchain sia

[545] Nakamoto nel white – paper "*Bitcoin: A Peer – to – Peer – Electronic Cash System"* spiega che l'elemento della fiducia è una debolezza del sistema, in quanto non si può negare il fatto che vi possano essere delle controversie e che le transazioni stesse non sono reversibili, oltre al fatto che i sistemi di pagamento tradizionali siano soggetti a frodi. Per approfondire si veda Nakamoto, 2008.

[546] (CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FG - BDLT), 2018)

composta da una pluralità di elementi che, se considerati singolarmente, sono dotati di determinate caratteristiche. A titolo di esempio, nonostante il Proof – of – Work e il Proof – of – Stake siano gli algoritmi di consenso maggiormente utilizzati nelle reti blockchain, nulla esclude che vi possano essere delle varianti o addirittura la creazione di nuovi protocolli di consenso, al fine di soddisfare le esigenze di utilizzo della blockchain in un determinato settore. Tali algoritmi, dunque, sono potenzialmente infiniti. In questo frangente sorge la necessità di standard tecnici che individuino regole o quantomeno linee guida affinché si possa affermare il modello tecnicamente migliore. Difatti, l'assenza di standard comporta al cc.dd. problema della salienza, ossia una tendenza dello sviluppo tecnologico per il quale sul mercato non si impone lo standard tecnicamente migliore, ma quello che riesce ad affermarsi maggiormente e a creare il maggior grado di dipendenza nell'ecosistema digito-sociale[547]. Sembra un controsenso, in quanto lo sviluppo tecnologico dovrebbe portare ad un progresso e all'affermarsi del modello migliore, ma considerati anche aspetti di carattere sociologico, culturale ed economico non è detto che ciò si verifichi[548]. Assenza di standard e salienza comportano conseguentemente ad un depotenziamento della tecnologia blockchain impedendo, quindi, di sfruttarne le migliori caratteristiche il che implica che per determinati settori il suo impiego non risulta essere la scelta migliore. Se si considera l'ambito elettorale è chiaro come esso debba essere adeguatamente regolamentato e come la blockchain debba adeguarsi a tale disciplina. In assenza si standard comuni, per uno Stato che decidesse di sperimentare la blockchain nel settore elettorale risulterebbe difficile effettuare una scelta tra le numerose proposte in materia, in quanto non si è sicuri che tale sia la scelta più adeguata. Non a caso, infatti, il modello di blockchain prevalente è quello originario, ossia il Bitcoin nonostante si siano evidenziate alcune criticità che hanno portato allo sviluppo di soluzioni alternative. Si potrebbe affermare come questa sfida possa essere superata con la individuazione di standard comuni. Se la soluzione fosse così semplice non si discuterebbe di tale problema. Vi è una difficoltà nell'individuare un pacchetto di regole condivise proprio perché la tecnologia blockchain è in continuo sviluppo, pertanto risulta essere uno sforzo alquanto impegnativo[549]. Nonostante ciò, si è cercato di individuare alcuni standard comuni in materia, affinché vi possa essere un maggior utilizzo di tale tecnologia[550]. La presenza di un set di regole comuni consente di evitare una frammentazione del settore, nonché dal punto di vista terminologico permette di avere una migliore comprensione della tecnologia in questione oltre al fatto che la presenza di standard aiuti anche a superare le criticità poste

[547] Sarra, 2022
[548] Per esempio, si potrebbe affermare come gran parte della popolazione utilizzi un determinato sistema operativo a discapito di un altro, il quale è più tecnicamente avanzato ma non è quello maggiormente utilizzato.
[549] Aristidou & Markou, 2019
[550] *Ibidem*

a livello della sicurezza e resilienza della blockchain[551]. A livello europeo nel 2018 si è dato vita ad un Focus Group, ossia il CENELEC[552], affinché fossero individuati i requisiti tecnici afferenti alle DLT e le blockchain. Si tratta, però, non di una normativa vera e propria ma di mere raccomandazioni. In particolare, come anche evidenziato dal BSI[553], anche il CENELEC condivide la necessità di individuare standard comuni al fine di evitare una frammentazione del settore consentendo, invece, un'interazione tra soggetti diversi affinché vi sia una creazione di un sistema funzionante[554]. Tutto ciò si traduce in una logica di mercato, ossia la presenza di regole condivise favorisce la competizione in quanto esse garantiscono l'interoperabilità, vale a dire la caratteristica per la quale diversi sistemi entrano in contatto tra loro superando la barriera della diversità[555]. Vista l'importanza di un set di regole comuni vi è da chiedersi quali siano. A livello internazionale, si può fare riferimento al comitato tecnico dell'ISO[556], ossia l'ISO/TC 307 rubricato *"Blockchain and distributed ledger technologies"* costituito nel 2016 il quale prevede una serie di proposte in materia come la classificazione degli smart contract, l'utilizzo della blockchain in nuovi settori o ancora i requisiti per migliorare, preservare e valutare la capacità di riservatezza delle DLT[557]. Sono tutti standard ancora in fase di sviluppo e approvazione, pertanto non vi è nulla di definitivo. È interessante osservare come dal 2016 ad oggi non si sia giunti ad un set di regole condivise, ma che il tutto sia ancora un *work in progress,* indice del fatto che ricercare standard comuni nella blockchain è più arduo di quanto sembri. Per quanto riguarda, invece, il CENELEC vi sono otto raccomandazioni, delle quali cinque risultano essere le più rilevanti. Per quanto attiene alla raccomandazione n.3, l'obiettivo è quello di raccogliere quante informazioni più possibili al fine di individuare le metodologie e software che possono essere utilizzati nella tecnologia blockchain in svariati settori, oltre al fatto che tali metodologie e programmi dovrebbero essere rilasciati *"in an open way",* ossia con un codice sorgente aperto[558], anche al fine di consentire a chiunque di utilizzare il software, di modificarlo e migliorarlo. Un altro problema che viene affrontato è quello previsto dalla raccomandazione n.4, ossia la questione energetica e l'impatto che tali tecnologie hanno sull'ambiente. Difatti è noto come la blockchain abbia un notevole impatto sull'ambiente causato principalmente dall'utilizzazione di computer dotati di elevato potere di calcolo per compiere le transazioni richieste. L'obiettivo, quindi, è quello di limitare le interazioni tra i device dell'Internet of Things allo stretto necessario[559]. Ulteriore aspetto che viene considerato è l'utilizzo

[551] BSI , 2017
[552] Acronimo per Comitato Europeo di normazione elettronica.
[553] Acronimo per British Standards Institution.
[554] CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FG - BDLT), 2018
[555] *Ibidem*
[556] Acronimo per International Organization for Standardization.
[557] Per approfondire si veda https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0
[558] CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FG - BDLT), 2018
[559] *Ibidem*

della blockchain nei servizi digitali di autenticazione. Vi è la necessità di predefinire il sistema o i sistemi di identificazione elettronica e la gestione delle identità registrate proteggendo allo stesso tempo i dati personali degli utenti, come previsto dalla raccomandazione n.5[560]. Tale è un aspetto assai rilevante per il voto elettronico che intende utilizzare la blockchain, in quanto la prima fase di ogni consultazione elettorale è l'identificazione dell'elettore. È assai notorio il fatto che vi sono diversi sistemi di autenticazione che spaziano dall'utilizzo di dati biometrici alla creazione di una coppia di chiavi pubbliche e private. Nel mare magnum di sistemi di identificazione digitale sarebbe, quindi, prospettabile la individuazione di un sistema uniforme per tutte le piattaforme di votazione elettronica che intendono utilizzare la blockchain in quanto ciò garantirebbe l'uniformità dell'apparato. La raccomandazione numero n.5, poi, rileva come sia necessario che la tecnologia blockchain garantisca anche la privacy degli utenti, in quanto vengono coinvolti diversi aspetti come il consenso dell'interessato, la legittimità dell'operazione, nonché la conservazione dei dati[561]. Per quanto riguarda il CENELEC, viene considerato questo aspetto fornendo una soluzione off – chain tale per cui i dati possono essere archiviati con un sistema peer – to – peer decentralizzato e non direttamente nel network. La raccomandazione n.6 è strettamente correlata alla precedente, ossia è necessario secondo il CENELEC considerare nella ricerca di standard anche il GDPR e tutte le sue implicazioni. Infine, l'ultima raccomandazione, ossia la n.8, suggerisce che sia necessario creare reti blockchain che siano interoperabili tra loro affinché possano essere utilizzati programmi e servizi governativi. In particolare, è raccomandata l'utilizzazione di interfacce standard per interagire con servizi esterni, oltre all'archiviazione dei dati in un formato standard affinché i dati possano essere trasferiti da blockchain a blockchain o da blockchain a servizi esterni garantendo, quindi, l'interoperabilità[562]. Non sono presenti solo progetti a livello *pubblico* circa la ricerca di standard in materia di blockchain, ma anche a livello privato chiaro indice di come anche le imprese necessitino di regole comuni affinché le potenzialità di tale tecnologia possano essere sfruttate al massimo. A titolo di esempio si può far riferimento a MOBI[563], ossia un'alleanza Web3 tra imprese che spaziano dal settore tecnologico a quello finanziario a quello della mobilità. In particolare con la comunicazione del luglio 2019 MOBI ha dato vita a *Mobility Open Blockchain,* ossia un'iniziativa che coinvolge i leader del settore automobilistico per lanciare nel mercato il primo VID[564] standard incorporante la tecnologia

[560] *Ibidem*
[561] A tal proposito si può citare lo studio condotto dal Parlamento Europeo nel 2019 relativo alla blockchain e al rispetto del GDPR, ossia il Regolamento n.679/2016 affrontando la tematica della compatibilità della rete blockchain con il GDPR considerato anche il difficile rapporto tra l'art.17 del GDPR statuente il cc.dd. diritto all'oblio con la caratteristica dell'immutabilità della blockchain. Per ulteriori approfondimenti si consulti EPRS - European Parliamentary Research Service, 2019
[562] CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FG - BDLT), 2018
[563] Per ulteriori informazioni si veda https://dlt.mobi/about/
[564] Acronimo per Vehicle Identification Device, ossia un sistema di identificazione digitale del veicolo.

blockchain affinché sia possibile tracciare la storia del veicolo considerando per esempio la manutenzione e il chilometraggio oltre che la produzione[565]. L'obiettivo è quello di favorire una condivisione dei dati tra le parti interessate inerenti al veicolo stesso e al suo ciclo di vita supportando i valori della trasparenza, cooperazione e automazione[566]. In conclusione si può affermare che nonostante vi sia stata la ricerca di standard in materia, al momento non è possibile individuare delle linee guida a livello generale essendo l'ambito della blockchain molto vasto. Il problema dell'assenza di standard, quindi, permane non consentendo di sfruttare al massimo le potenzialità della blockchain. Una soluzione che si potrebbe prospettare in tal senso è quella di una ricerca di linee guida minime di settore senza avere, dunque, la pretesa di individuare standard a carattere generale che siano validi per qualsiasi ambito di utilizzo della blockchain in quanto ognuno di esso è diverso e necessita il soddisfacimento di esigenze diverse.

4.2.Il problema della scalabilità

Si è osservato come l'assenza di standard sia un problema che ad oggi risulta essere ancora irrisolto. Vi sono state varie proposte, come ad esempio le raccomandazioni del CENELEC o progetti privati come il MOBI, ma emerge una difficoltà di individuare delle linee guida generali poiché il settore tecnologico e in particolare quello della blockchain è molto vasto, pertanto individuare un set di regole comuni risulta operazione alquanto complessa, posto che non è detto che gli standard comunque individuati siano applicabili e adatti nei settori in cui la blockchain intende essere utilizzata. Ulteriore sfida che la blockchain pone è il cc.dd. problema della scalabilità, il quale in letteratura presenta una vasta rosa di soluzioni che nel concreto rende difficile individuare quale sia la migliore per risolvere tale problematica. Si propone, quindi, anche in questo caso come nell'assenza di standard la questione della salienza. Si può affermare, infatti, che nonostante siano presenti numerose proposte per superare la scalabilità, non è detto che si affermi la soluzione migliore o quella più tecnicamente avanzata. Venendo alla definizione di scalabilità, essa si riferisce alla capacità della rete blockchain di gestire un numero sempre più crescente di transazioni. Più nello specifico, all'aumentare del numero delle transazioni la blockchain dovrebbe mantenere lo stesso livello di prestazioni. La scalabilità viene misurata considerando il *transaction throughput latency,,* ossia il valore che indica la velocità con cui un blocco viene processato e aggiunto alla catena[567]. Tale valore dipende dalla grandezza del blocco[568]

[565]https://dlt.mobi/mobi-announces-the-first-vehicle-identity-vid-standard-on-blockchain-in-collaboration-with-groupe-renault-ford-and-bmw-among-others/
[566] *Ibidem*
[567] Sanka & Cheung, 2021
[568] È il valore che indica il numero massimo di transazioni che il blocco può accogliere e il numero di informazioni ad esso associate. Tratto da Nasir, et al., 2022

e dal cc.dd. *block time*[569]. La scalabilità, inoltre, può essere considerata in senso orizzontale e verticale. Il primo concetto si riferisce alla capacità della blockchain di espandere la rete di partecipanti aggiungendo nuovi nodi al network. L'obiettivo è quello di incrementare l'ampiezza della rete senza compromettere l'efficienza e le prestazioni della blockchain[570]. Per scalabilità verticale, invece, si fa riferimento alla capacità dei nodi partecipanti alla rete di raggiungere elevati livelli in termini di prestazioni concentrandosi, quindi, su alcuni elementi della blockchain come la grandezza dei blocchi[571]. L'origine del problema della scalabilità risiede nelle riflessioni effettuate circa il Bitcoin e il suo protocollo di consenso, ossia del Proof – of – Work, in quanto all'interno della catena viene creato un nuovo blocco ogni dieci minuti e la grandezza del blocco è pari ad un mega byte[572]. È chiaro che tale algoritmo di consenso non sia in grado di sostenere un numero elevato di transazioni. Il problema della scalabilità è compreso in quello che nel gergo viene chiamato *the blockchain trilemma,* ossia scalabilità, decentralizzazione e sicurezza non possono coesistere senza che una di queste proprietà venga compromessa[573]. Se si considera la blockchain privata, infatti, la sicurezza e la scalabilità coesistono, ma a discapito della decentralizzazione. La decentralizzazione in questa tipologia di blockchain viene sacrificata, per così dire, in quanto affinché per poter partecipare al network è necessario essere dotati dell'autorizzazione proveniente da un'autorità terza che funge da *gatekeeper* in quanto solo chi soddisfa determinati requisiti, previsti dalla blockchain, vi può fare parte. Se si considera, invece, la rete *permissionless,* ossia pubblica viene garantita la sicurezza e la decentralizzazione, ma si pone il problema della scalabilità[574]. Difatti, la rete pubblica è accessibile a tutti, pertanto essa sarà molto più estesa rispetto alla blockchain *permissioned*[575] e in caso di aggressione informatica qualora più nodi non dovessero funzionare, tutti gli altri fungerebbero da *backup* in quanto detengono una copia di tutte le transazione effettuare nella rete. La scalabilità è rilevante nel voto elettronico, in quanto pur essendo una problematica di carattere squisitamente tecnico influenza l'andamento delle consultazioni elettorali. Difatti, per le consultazioni di modeste dimensioni, come le elezioni amministrative, tale problematica non si dovrebbe porre poiché il numero di transazioni risulta essere sopportato dalla blockchain e pertanto viene mantenuta la sua efficienza. Si pone, invece, per le consultazioni di dimensioni più vaste, come le elezioni per la rinnovazione del Parlamento, essendo una consultazione molto più ampia e pertanto non si esclude che il numero delle transazioni effettuate sia particolarmente elevato. Ciò comporta non solo a dover sfruttare una

[569] È il valore che indica con quale frequenza viene prodotto un nuovo blocco nella rete.
[570] Nasir, et al., 2022
[571] *Ibidem*
[572] Zhou, Huang, Zheng, & Bian, 2020
[573] Sanka & Cheung, 2021
[574] *Ibidem*
[575] Ossia la blockchain privata.

blockchain che sia in grado di mantenere elevate prestazioni all'aumentare del carico di lavoro, ma anche a fronteggiare problemi inerenti alla sicurezza, come accennato nel *blockchain trilemma*, e all'affidabilità della rete stessa in quanto vi è la necessità di evitare la circostanza per la quale all'aumentare del carico di lavoro vi siano interruzioni di servizio che comportano ad un malfunzionamento del network. Questo aspetto implica, dunque, la necessità di comprendere che cosa succede qualora si presentasse un malfunzionamento del sistema e quale sia la sorte dei voti espressi. Facendo una breve considerazione sul punto, si potrebbe affermare che qualora si dovesse utilizzare un rete *permissionless* non si porrebbero problemi, in quanto tutte le transazioni sono registrate dai nodi nella rete, pertanto se qualcheduno non dovesse funzionare vi sarebbe comunque una copia delle operazioni effettuate. Si è visto però come la rete privata sia quella maggiormente utilizzata dalle piattaforme di votazione elettronica, in quanto consente solo agli elettori specificatamente individuati nelle liste elettorali di accedere alla rete superando così il *gatekeeper* della rete. Essendo una rete di dimensioni ridotte, qualora più nodi fossero sottoposti ad un attacco informatico il numero di *peers* che detengono una copia delle operazioni effettuate è ridotto drasticamente, pertanto risulterebbe difficile recuperare le preferenze finora espresse. Questo comporta, dunque, la necessità di garantire adeguati sistemi di sicurezza e soprattutto considerare il voto elettronico come una forma aggiuntiva di espressione del suffragio e non sostituiva della modalità tradizionale. Al di là di queste considerazioni, al problema della scalabilità si è cercato di dare più soluzioni, le quali possono essere principalmente raggruppate in soluzioni *on chain* e *off chain.* Le soluzioni *on chain* hanno come obiettivo quello di migliorare alcuni parametri ed elementi della rete. Ad esempio, per fronteggiare il carico di lavoro si potrebbe pensare ad un aggiustamento dei blocchi nel senso di una loro compressione riducendo il quantitativo di dati che un singolo blocco è in grado di archiviare agendo sull'intestazione del blocco, ossia l'*header* e le transazioni stesse le quali sarebbero delle *short transactions* contenenti un ID specifico corrispondente a una determinata transazione che è già disponibile per chi la riceve. In sostanza, si considerano due nodi A e B. Il nodo A invia un blocco *compattato* al nodo B, il quale dovrebbe essere in grado di calcolare il codice di transizione, ossia il TXID, di tutte le operazioni presenti nel suo *pool.* Una volta trovato il TXID, esso viene fatto corrispondere a quelli presenti nel blocco *compattato*. Successivamente, se tutte le transazioni in sospeso sono disponibili nel nodo B si procederà alla creazione dell'intero blocco[576]. Se tale soluzione risultasse un po' laboriosa e complessa si potrebbe optare per una modifica dei presenti algoritmi di consenso. Ad esempio, il Proof – of – Work presenta numerose varianti, tra cui il Bitcoin – NG. Secondo questo protocollo di consenso, il tempo viene diviso in epoche ognuna delle quali ha un suo

[576] Zhou, Huang , Zheng , & Bian, 2020

leader. Il leader ha il compito di serializzare le transazioni effettuare e per facilitare tale operazione sono presenti due blocchi, ossia i *key blocks* per l'elezione del leader e i *microblocks* i quali, invece, registrano tutte le operazioni effettuare nella rete[577]. Le soluzioni *off – chain,* invece prevedono l'esecuzione di transazioni all'esterno della rete blockchain in modo da ridurre il carico di lavoro della rete "principale"[578]. Tra le soluzioni più celebri vi è il cc.dd. *sharding*, ossia una tecnica per la quale i dati contenuti in un database vengono suddivisi in più frammenti e archiviati in diversi servers per ridurre il carico di lavoro del server centrale. Lo stesso è possibile effettuarlo con la blockchain, ossia è possibile suddividere l'intera rete in più network contenenti un certo numero di nodi detti *shard*. In questo modo viene affrontato il problema della scalabilità garantendo allo stesso tempo un elevato livello di prestazioni[579]. È una soluzione che consentirebbe di risolvere la scalabilità, ma allo stesso tempo pone delle questioni inerenti alla sicurezza della rete. La forza della tecnologia blockchain, infatti, consta nel fatto che è una rete *peer – to – peer* e come detto nel corso della trattazione, anche se più nodi non dovessero funzionare non si porrebbero problemi, in quanto tutti gli altri fungono da rete di sostegno detenendo una copia di quanto effettuato nella rete. Se si suddivide la rete in più network la sicurezza della rete stessa potrebbe essere compromessa e vi potrebbero essere attacchi come il double spending[580], ossia una transazione fraudolenta per cui un soggetto cerca di spendere un certo ammontare di denaro nella stessa rete per due volte. Questo si potrebbe verificare, in quanto, anche se presenti più reti che in apparenza potrebbero essere considerate diverse l'una dall'altra, in realtà appartengono tutte alla stessa rete. Traendo le conclusioni è constatato che la tecnologia blockchain sia molto promettente e una delle innovazioni più rilevanti nell'ultimo decennio. In origine, il suo campo di applicazione era strettamente limitato alla finanza ma si compresero fin da subito le potenzialità di tale innovazione al punto di sperimentarne l'utilizzo in diversi ambiti, tra cui quello elettorale. Si è visto, però, come nonostante l'idea sia promettente vi siano alcuni ostacoli sia di carattere giuridico sia di carattere tecnico. Nulla vieta di pensare, però, che in un futuro prossimo queste difficoltà possano essere superate grazie allo sviluppo tecnologico da un lato e dall'altro ad un certo interesse per il Legislatore verso nuove prospettive di utilizzo della tecnologia nel diritto.

[577] Eyal, Gencer, Gun Sirer, & van Renesse, 2016
[578] Nasir, et al., 2022
[579] Zhou, Huang , Zheng , & Bian, 2020
[580] *Ibidem*

Conclusioni

La proposta di utilizzare la tecnologia blockchain nel voto elettronico è promettente e interessante, ma come si è visto vi sono alcuni ostacoli che al momento ne inibiscono l'utilizzazione.

Il primo ostacolo che rallenta, per così dire, l'implementazione del voto elettronico su blockchain è di carattere tecnico. Vi è infatti una difficoltà nel creare un sistema di votazione elettronica adeguato, in quanto vi è la necessità di compiere determinate scelte che risultano essere rilevanti per lo svolgimento delle consultazioni elettorali. In primis, a seconda dell'algoritmo di consenso utilizzato si pone il problema della scalabilità che, come si è visto, è una delle criticità sollevate in materia. La rete deve essere in grado di sopportare un elevato carico di lavoro e allo stesso tempo garantire l'efficienza delle prestazioni e la sicurezza che sono alcune delle caratteristiche che contraddistinguono questa tecnologia. Vi è, quindi, la necessità di selezionare il protocollo di consenso più adattato anche alla *grandezza* delle consultazioni elettorali. Al momento sono presenti varie soluzioni sia *on chain* sia *off chain* che consentirebbero di superare questo ostacolo. In secondo luogo, per quanto riguarda la tipologia di blockchain utilizzata si è constatato come la rete pubblica, detta *permissionless*, nonostante sia maggiormente resiliente alle aggressioni informatiche non esclude il rischio di essere utilizzata per fini malevoli. Difatti, essendo una rete aperta chiunque vi può accedere e sfruttare la blockchain per operazioni criminose essendo tutelato dall'anonimato dal momento che l'identità di chi effettua le transazioni non è rivelata. A fronte di questi limiti, quindi, la rete privata, ossia *permissioned,* risulta essere più adeguata, in quanto consente solo a chi ha ottenuto l'autorizzazione da parte del network di accedervi e pertanto vi è un maggior controllo sui partecipanti. Allo stesso tempo, però, essendo una rete fortemente centralizzata ciò espone tale tipologia di blockchain a probabilità più elevate di essere vittima di attacchi informatici.

Dal punto di vista giuridico si è osservato come i principi espressi in materia a livello sovranazionale con le Raccomandazioni del Consiglio d'Europa del 2004 e del 2017 pongono delle linee guida, e non principi veri e propri, che nella loro formulazione risultano essere di respiro più ampio rispetto a quanto espresso dall'articolo 48 della Costituzione, pertanto l'utilizzo della blockchain nel voto elettronico in questa prospettiva risulta possibile. Se si guarda, invece, all'ordinamento interno si è constatato come i principi di personalità, eguaglianza, libertà e segretezza sono irrinunciabili, poiché a presidio dell'esercizio del diritto al voto. Ci si è posti, però, una domanda, ossia se non sia il momento di modificare il dettato costituzionale per aprire le porte a nuove sperimentazioni in materia, constatato

il fatto che con il disegno legge n.1323 della XVIII Legislatura vi era stata un'apertura all'utilizzo di sistemi di votazione elettronica su blockchain con riferimento al voto per corrispondenza per i cittadini italiani all'estero. La risposta a questo quesito è difficile da dare. Da un lato i principi espressi dall'articolo 48 della Costituzione sono a presidio dell'esercizio del diritto al voto, il quale è una delle manifestazioni più rilevanti della sovranità popolare. Difatti, l'articolo 1 e l'articolo 48 della Costituzione vengono letti in combinato disposto. Dall'altro lato, però, bisogna prendere atto di come i tempi stiano cambiando e di come in un futuro, neanche tanto prossimo, si possa pensare di sperimentare e utilizzare la tecnologia blockchain nel settore elettorale. Il tutto si riduce ad un bilanciamento tra innovazione e tradizione.

In conclusione si può affermare che pur essendoci una necessità di innovazione e ammodernamento all'interno del settore elettorale, anche per far fronte alla perdurante crisi della democrazia rappresentativa, è chiaro come allo stato attuale difficilmente potrà avere successo l'utilizzo di sistemi di votazione elettronica basati su blockchain. L'espressione del suffragio con la modalità tradizionale, infatti, al momento risulta essere il sistema migliore e non pone tutte le problematiche che, invece, il voto elettronico e la blockchain mettono in luce. Questo, però, non implica che gli studi in materia debbano essere abbandonati. Vi deve essere una costante ricerca di innovazione per guardare al futuro e cogliere le opportunità e i vantaggi che tale tecnologia offre.

Bibliografia

Risoluzione del Parlamento europeo del 16 marzo 2017 sulla e-democrazia nell'Unione europea: potenziale e sfide (2016/2008(INI)).

§1 Telecommunication Act (2000)

§5 Local Government Council Election Act (2002)

Ahmad, H., Tabassum, F. N., Ayaz, S. A., Bahir, N., & Meelam, M. (2021). Electronic voting system: nature, origin and its global application. *International Journal of Innovation, Creativity and Change, 15*(2), 1334 - 1337.

Alatawi, F., Cheng , L., Tahir , A., Karami , M., Jiang , B., Black , T., & Liu, H. (2021). A survey on echo chambers on social media: description, detection and mitigation. 1-21. Tratto da https://arxiv.org/abs/2112.05084

Amoretti , F., & Santaniello , M. (2021, aprile). Partecipazione politica e opinione pubblica online in tempo di crisi. *Iride*, p. 57-67. doi:10.1414/101251

Aristidou , C., & Markou , E. (2019). Blockchain Standards and Government Applications. *Journal of ICT Standardization, 7*(3), 287 - 312. doi:0.13052/jicts2245-800X.736

Arslan, C., Sipahioğlu, S., Şafak, E., Gözütok, M., & Köprülü, T. (2021). Comparative Analysis and Modern Applications of PoW, PoS, PPoS Blockchain Consensus Mechanisms and New Distributed Ledger Technologies. *Advances in Science, Technology and Engineering Systems Journal, 6*(5), 279 - 290. doi:DOI: 10.25046/aj060531

Articolo 1 co. 107 - 114 Legge n.160/2019

Articolo 1 co.627 Legge n.160/2019

Articolo 1 co.628 Legge n.160/2019

Articolo 1 d.l. n.49/2008 conv. legge n.96/2008

Articolo 1 Dichiarazione Universale dei diritti dell'uomo (1948)

Articolo 1 Direttiva n.243/2018.

Articolo 1 Legge 25 gennaio 1982 n.17

Articolo 1 Legge 9 febbraio 1963 n.63

Articolo 1106 Codice civile. (1865)

Articolo 115 DPR n.361/1957

Articolo 12 co.1 lett. e); lett. f) disegno di legge n.1313 XVIII Legislatura. Tratto da https://www.senato.it/japp/bgt/showdoc/18/DDLPRES/0/1114477/index.html?part=ddlpres_ddlpres1-articolato_articolato1

Articolo 12 Legge 27 dicembre 2001 n.459

Articolo 15 co.1 TFUE

Articolo 2 Dichiarazione dei diritti in Internet

Articolo 7 TUE

Articolo 70 DPR n.361/1957

Articolo 71 DPR n.261/1957

Articolo 73 DPR n.361/1957

Articolo 75 DPR n.361/1957

Articolo 83 DPR n.361/1957

Articolo 8-ter d.l. n.135/2018 conv. Legge 11 febbraio 2019 n.12

Articolo 9 legge 4 aprile 1956 n.212

Awad , M., & Leiss, E. L. (2016). The Evolution of Voting: Analysis of Conventional and Electronic Voting Systems. *International Journal of Applied Engineering Reasearch, 11*(12), 7892.

Azaria, A., Ekblaw, A., Vieira , T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2nd International Conference on Open and Big Data*, (p. 25-30). Cambridge, Massachussets. doi:10.1109/OBD.2016.11

Bassanini, F. (2022). Tratto da Libro bianco sull'astensionismo - Per la partecipazione dei cittadini: come ridurre l'astensionismo e agevolare il voto: https://www.riformeistituzionali.gov.it/it/comunicazione/comunicati-stampa/presentato-il-libro-bianco-sullastensionismo/

Bayan , T., & Banach , R. (4-6 May 2023). Exploring the privacy concerns in permissionless blockchain networks and potential solutions. Astana, Kazahstan: IEEE Smart Information Systems and Technologies (SIST). doi:https://doi.org/10.48550/arXiv.2305.01038

Benabdallah , A., Audras , A., Coudert , L., El Madhoun , N., & Badra , M. (2022, July 11th). Analysis of Blockchain Solutions for E-voting: a systematic literature review. *IEEE Access*, 7746 - 77059. doi:10.1109/ACCESS.2022.3187688

Bettinelli, E. (1990). Diritto di Voto. In *Digesto* (Vol. V, p. 217 - 232). UTET.

Bettinelli, E. (2022). La lunga marcia del voto elettronico in Italia. *Italian Journal of Electoral Studies (IJES), 46*(1), 5-48. doi:https://doi.org/10.36253/qoe-12775

Bishr, A. B. (2019). Dubai: a City Powered by Blockchain. *Innovations: Technology, Governance, Globalization*, 1-5. doi:https://doi.org/10.1162/inov_a_00271

Bobbio, N. (1984). *Il futuro della democrazia.* Einaudi.

Brotsis, S., Kolokotronis, N., Limniotis, K., Bendiab, G., & Shiaeles, S. (2020). On the security and privacy of Hyperledger Fabric: challenges and open issues. *IEEE World Congress on Services*, (p. 197 - 204). doi:10.1109/SERVICES48979.2020.00049

Bruschi , D., Rusconi , D., & Zoia , M. (2022, settembre). La diversificazione delle tecnologie blockchain. *Osservatorio del diritto civile e commerciale*, 9 - 22 . doi:10.4478/106697)

Camon, A. (2021). In A. Camon , C. Cesari , M. Daniele , M. Di Bitonto , D. Negri , & P. Paulesu, *Fondamenti di procedura penale* (p. 103 - 104). Vicenza: Wolters Kluwer.

Chan, C., Zhao , M., & San Lee , P. (2023). Determinants of escape from echo chambers: the predictive power of political orientation, social media use, and demographics. *Global media and China, 8*(2), 155 -173. doi:https://doi.org/10.1177/20594364221140820

Commissione delle comunità europee. (2003, settembre 26). Il ruolo dell'eGovernment per il futuro dell'Europa. *COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE*. Bruxelles .

Coniglione, C. (2023). L'utilizzo dei big data in ambito politico-elettorale e il loro impatto sulla democrazia rappresentativa. *Nomos*, 2-3. Tratto da https://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2023/06/coniglione.note1-2023.pdf

Corte costituzionale. (2014, gennaio 15). *Sentenza n.1/2014*. Tratto da https://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2014&numero=1

Corte Costituzionale sentenza n.43/1961

Council of Europe. (2004). Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting. Tratto da https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp

Council of Europe. (2017). Recommendation CM/Rec(2017)5 of the Committe of Ministers to member States on standards for e-voting. Tratto da https://rm.coe.int/0900001680726f6f

Cuolo, L. (2019). Le forme di Stato. In T. E. Frosini (A cura di), *Diritto pubblico comparato. Le democrazie stabilizzate* (p. 104-106). Bologna: Il Mulino.

Dahlgren, P. M. (2021). A critical review of filter bubbles and a comparison with selective exposure. *Nordicom Review, 42*(1), 15 - 33. doi:10.2478/nor-2021-0002

De Gregorio, G. (2019). The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online? *MediaLaws*, 95. Tratto da https://www.medialaws.eu/wp-content/uploads/2019/05/9.-De-Gregorio.pdf

Desantis, V. (2022, ottobre 27). Le nuove prospettive dell'Internet voting tra avanzamento tecnologico e sostenibilità giuridica. *AIC, Associazione italiana costituzionalisti*(4), 47 -64.

Diaz Ruiz, C., & Nilsson , T. (2023). Disinformation and echo chambers: how disinformation circulates on social media through identity - driven controversies. *Journal of public policy and marketing, 47*(1), 18 -35. doi:https://doi.org/10.1177/07439156221103852

Diedrich, D. (2020). Distributed Ledger Technologies. *Georgetown Law Tecnhology Review*, 673 - 683. Tratto da https://georgetownlawtechreview.org/wp-content/uploads/2020/07/4.2-p673-683-Diedrich.pdf

Direttiva 2009/110/CE del Parlamento europeo e del Consiglio concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/4. (2009, settembre 16). Tratto da https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:IT:HTML

Dubois, E., & Black, G. (2018, January 29th). The echo chamber is overstated: the moderating effect on political interest and diverse media. *Communication and society, 21*(5), 729 - 745. doi:https://doi.org/10.1080/1369118X.2018.1428656

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022, giugno 16). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*, 1-14. doi:https://doi.org/10.1016/j.giq.2022.101718

El Ioini, N., & Pahl, C. (2018). A Review of Distributed Ledger Technologies. *On the Move to Meaningful Internet Systems. OTM 2018 Conferences. 11230*, p. 1-13. Bolzano: Springer Cham. doi:https://doi.org/10.1007/978-3-030-02671-4_16

Emre, A. (2022). Can Blockchain Technology Increase Participation in Local Goverments? A Review on Blockchain - based Voting Systems in Local Governments. *R&S - Research Studies Anatolia Journal, 1*(5), 121 - 147. Tratto da https://www.ceeol.com/search/article-detail?id=1016468

EPRS - European Parliamentary Research Service. (2019). Blockchain and The General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? doi:10.28617/535

Eyal, I., Gencer, A., Gun Sirer, E., & van Renesse, R. (2016). Bitcoin - NG: A Scalable Blockchain Protocol. *Usenix - The advanced computing systems association*, 45 - 59. Tratto da https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf

Eysenbach, G. (2001). What is e-health. *Journal of medical internet research*, 1-2. doi:10.2196/jmir.3.2.e20

Faini, F. (2020). Blockchain e diritto: la "catena del valore" tra documenti informatici, smart contracts e data protection. *Responsabilità civile e previdenza*, 297 - 316. Tratto da https://publicatt.unicatt.it/handle/10807/191968

Farahani, B., Firouzi, F., & Luecking, M. (2020, December 17). The convergence of IoT and distributed ledger technologie (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications*. doi:https://doi.org/10.1016/j.jnca.2020.102936

Ferrajoli, L. (2014, Dicembre). I diritti fondamentali come dimensione della democrazia costituzionale. *Ricerche giuridiche, 3*(2), 211 - 222. Tratto da https://edizionicafoscari.unive.it/media/pdf/article/ricerche-giuridiche/2014/6/i-diritti-fondamentali-come-dimensioni-della-democ/art-missing-article-doi.pdf

Ferrari, G. F. (2015, Luglio - Settembre). Partiti antipartito e partiti antisistema: nozione e tipologie alla prova del diritto contemporaneo. *Diritto pubblico comparato ed europeo*(3).

Floridia, A. (2015, maggio - agosto). La rete, la sfera pubblica e i luoghi della deliberazione pubblica. *Iride, 28*, p. 321-330. doi:10.1414/80569

Fornasier, M. D. (2021). The Realization of E-Democracy in the 21st Century. *Revista da Facultade de Deireto da Universidade Federal de Minas Gerais*, 259-284. doi:10.12818/P.0304-2340.2021 v78p259

Frosini, T. E. (2017). Internet e democrazia. *Il diritto dell'informazione e dell'informatica, 4*(5), p. 657-671.

Gallo, F. (2020, marzo 20). DEMOCRAZIA 4.0. LA COSTITUZIONE, I CITTADINI E LA PARTECIPAZIONE. *Associazione italiana costituzionalisti*, p. 487-500. Tratto da https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/franco-gallo/democrazia-4-0-la-costituzione-i-cittadini-e-la-partecipazione

Garante della protezione dei dati personali. (2017, dicembre 21). Provvedimento n.548 su data breach.

Garante per la protezione dei dati personali. (2019, aprile 4). Provvedimento n.83 sul data breach.

Gauthier, L. (2023). A Brief Overview of the Political Economy of Ancient Greek Polis and Demokratia. *Investigaciones de Historia Económica - Economic History Research*, 2-4. doi:https://doi.org/10.33231/j.ihe.2023.05.002

GENÇOĞLU1, M. T. (2022). Mathematical Analysis of The Hash Functions as a Cryptographic Tools for Blockchain. *Turkish Journal of Science & Technology*, 197-201. doi:https://doi.org/10.55525/tjst.1140811

Gometz , G., & Tawa , M. (2018). Voto elettronico presidiato e blockchain. *Ragion Pratica*(2), 317-328. doi:10.1415/91541

Gometz, G. (2017). *Democrazia elettronica. Teoria e tecniche.* Edizioni ETs.

Guggenberger, T., Sedlmeir, J., Fridgen, G., & Luckow, A. (2022). An in-depht investigation of the performance characteristics of Hyperledger Fabric. *Computers & Industrial Engineering*, 1 - 20. doi:https://doi.org/10.1016/j.cie.2022.108716

Guven, A. (2020). The Challenges of Electronic Votinng in Terms of Constitutional Parameters: Case of Estonia and Germany. *International Journal of Social Sciences*, 79-93.

Haber, S., & Stornetta, W. (1991). How To Time-Stamp a Digital Document. *Journal of Cryptology*, 99 - 111. doi:https://doi.org/10.1007/BF00196791

Haroon-Sulyman, S. (2014, January). Client-Server Model. *IOSR Journal of Computer Engineering* , 67-71. doi:DOI: 10.9790/0661-16195771

Hobolt , S., Lawall , K., & Tilley , J. (2023). The polarizing effect of partisan echo chambers. *American political science review*, 1 -16. doi:doi:10.1017/S0003055423001211

Hossain Faruk, M., Aman , F., Islam , M., & Rahman , A. (2024, April 19th). Transforming online voting: a nove system usign blockchain and biometric verification fo enhanced security, privacy and trasparency. *Cluster Computing*. doi:https://doi.org/10.1007/s10586-023-04261-x(0123456789().,-volV)(0123456789().,-volV)

Ibba , S., Pinna, A., Seu, M., & Pani, F. (2017). CitySense: blockchain-oriented Smart Cities., (p. 1-5). Cologne, Germany.

Imetaj, A., Amini, M., & Pardalos, P. (2021). *Foundations of Blockchain. Theory and Applications.* Springer. doi:https://doi.org/10.1007/978-3-030-75025-1

Innocent, U. U. (2018). Wireless networking using peer - to - peer.

Isastia, A. (2008). La battaglia per il voto nell'Italia liberale. *Dal diritto di voto alla cittadinanza piena*, 31-51. doi:10.1400/103354

Khan , S., Shael , M., Majdalawieh , M., Nizamuddin, N., & Nicho , M. (2022). Blockchain for Governments: The Case of the Dubai Government. *Sustainability*, 11 - 15. doi:https://doi.org/10.3390/su14116576

Kiayias , A., & Yung , M. (2002). Sel-tallying Election and Perfect Ballot Secrecy. *International Workshop on Public Key Cryptography. 2274*, p. 141 - 158. Paris: Springer. doi:https://doi.org/10.1007/3-540-45664-3_10

Legge 15 gennaio 1991 n.15

Legge 7 agosto 1990 n.241

Legge 22 gennaio 1882 n. 999

Legge 30 giugno 1912 n.666

Legge 17 marzo 1848 n.689

Lepore , C., Ceria , M., Visconti, A., Pratap Rao , U., Arvindbhai Shah , K., & Zanolini , L. (2020). A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. *Mathematics*, 1-26. doi:10.3390/math8101782

Li, P., Feng, W., Yan , Z., Li, Y., Zhou , X., & Shimizu , S. (2021). Privacy preservation in permissionless blockchain: a survey. *Digital communications and networks*, 295 - 307. doi:https://doi.org/10.1016/j.dcan.2020.05.008

Lu , Y., Li , H., Gao , L., Yu, J., Yu, Y., & Su, H. (2023). Self-tallying e-voting with public traceability based on blockchain. *Computer Standards & Interfaces, 88*(103795), 1-13. doi:https://doi.org/10.1016/j.csi.2023.103795

M. Ghazal, T., Al Hmmadi, M., Kamran, R., Kamrul Hasan, M., Al-Dmour , N., Alzoubi , H., . . . Mago , B. (2022). Securing Smart Cities Using Blockchain Technology. *1st International Conference on AI in Cybersecurity*, (p. 2).

Magna Charta 1215. (s.d.). Tratto da https://my.liuc.it/MatSup/2017/L14204/Magna_Charta.pdf

Makani , S., Pittala, R., Alsayed, E., Aloqaily , M., & Jararweh, Y. (2022). A survey of blockchain applications in sustainable and smart cities. *Cluster Computing*, 3918-3919. doi:https://doi.org/10.1007/s10586-022-03625-z(0123456789().,-volV)(0123456789().,-volV)

Marchettoni, L. (2018). *Breve storia della democrazia. Da Atene al populismo* (Vol. 8). Firenze: Firenze University Press. Tratto da http://digital.casalini.it/9788864537610

Matinovic , I., Kello , L., & Sluganovic , I. (2017). Blockchains for Governmental Services: Design Principles, Applications, and Case Studies. *Center for technlogy & global affairs*, 8 -13. Tratto da https://www.politics.ox.ac.uk/sites/default/files/2022-03/201712-CTGA-Martinovic%20I-Kello%20L-blockchainsforgovernmentalservices.pdf

Mazzola, R. (XVI, 2019). Note su Internet e democrazia. *Laboratorio dell'ISPF*, 1-14. doi:10.12862/Lab19MZR

Mazzucca, J. (2023). Women in Law. Un'eccezione alla regola. Il diritto negato di Lidia Poet, e non solo. In I. Dossier (A cura di), *Le ispirazioni del giurisita*, *16*, p. 11. Campobasso. doi:10.6092/unibo/amsacta/7226

McCorry , P., Shahandashti , S. F., & Hao , F. (2017). A smart contract for boardroom voting with Maximum Voter Privacy. *21st International Conference on Financial Cryptography and Data Security*, (p. 357 - 375). Sliema. doi:10.1007/978-3-319-70972-7_20

Merkle, R. (1978). Secure Communictations Over Insecure Channels. *Programming Techniques*, 294-299. Tratto da https://citeseerx.ist.psu.edu/doc/10.1.1.364.5157

Milani, G. (2019). Parlamento e parlamentarismo nella democrazia illiberale: l'esperienza ungherese. *DPCE online, 4*, 2837. doi: http://dx.doi.org/10.57660/dpceonline.2019.840

Mojtaba , S., Bamakan , H., Motavali, A., & Babei Bondarti , A. (13th April 2020). A survey of blockchain consensus algorithms perfomance evaluation criteria. *Expert Systems with applications*, 9-19. doi:https://doi.org/10.1016/j.eswa.2020.113385

Montaldo, R. (2019, Dicembre 4). Le dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali. *Quaderni costituzionali* (4), p. 789-810. doi:10.1439/95226

Moro, Paolo. (2021). Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa. In P. Moro (A cura di), *Etica, diritto e tecnologia* (p. 9). Franco Angeli.

Movimento 5 Stelle. (2021). Nuovo Statuto 2021. Tratto da https://www.movimento5stelle.eu/wp-content/uploads/2021/07/NUOVO-STATUTO-TESTO-DEFINTIVO.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Chash System. 1-9. Tratto da https://bitcoin.org/bitcoin.pdf

Namasudra, S., & Akkaya, K. (2023). Introduction to Blockchain Technology. In S. Namasudra, & K. Akkaya , *Blockchain and its Apllications in Industry 4.0. Studies in big data* (Vol. 119). Springer. doi:https://doi.org/10.1007/978-981-19-8730-4_1

Nasir, M. H., Arshad , J., Khan, M. M., Fatima, M., Salah, K., & Jayraman, R. (2022). Scalable blockchains - A systematic review. *Future Generation Computer Systems*, 136 - 162. doi:https://doi.org/10.1016/j.future.2021.07.035

Ordinanza, RG 59264/2019 (Roma dicembre 12, 2019). Tratto da https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/01/sentenzacpifb.pdf

Papanikos, G. T. (2017). *Democracy in Acient Athens and in the Contemporary World.* Athens Institute for Education and Research (ATINER), Athens.

Parlamento Europeo. (2018, ottobre 3). Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione. Tratto da https://www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.html

Phadke, A., Medrano, F., & Ustymenko, S. (2022). Applications of Blockchain in E-government. *2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE)*, (p. 157-164). doi:10.1109/ISEEIE55684.2022.00035

Piraino, A. (2020). Crisi della democrazia, taglio dei parlamentari e trasformazioni del sistema delle leggi elettorali. *Federalismi.it*, 1-19. Tratto da https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41982

Pisaneschi, A. (2018). Norme giuridiche e fonti del diritto. In A. Pisaneschi, *Diritto Costituzionale* (p. 64). Torino: Giappichelli .

Politou , E., Casino, F., Alepis , E., & Patsakis , C. (2019). Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing , 9*, 1972 - 1986.

Raniolo , F., & Tarditi , V. (2021, maggio-agosto). La rivoluzione digitale e le trasformazioni organizzative dei partiti. *Rivista di Digital Politics*, p. 249-270. doi:10.53227/101942

Raniolo, F. (2020). Verso democrazie illiberale e oltre. *DPCE online, 3*, 3914 - 3915. doi: http://dx.doi.org/10.57660/dpceonline.2020.1098

Rivera, I. (2017). La Rete, i populismi e i partiti politici 2.0. *Informatica e diritto, 1*(2), 274 - 278.

Rospi, M. (2021). La tutela del diritto al voto come argine alle diseguaglianze dopo l'emergenza pandemica. *PA Persona e Amministrazione, IX*(2), 227 - 259. Tratto da https://journals.uniurb.it/index.php/pea/article/view/3316

S. Alnahari , M., & T. Ariaratnam, S. (2022). The Application of Blockchain Tecnhology to Smart City Infrastructure. *Smart cities*, 988. doi:https://doi.org/10.3390/smartcities5030049

Sanka , A., & Cheung , R. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications, 125*, 1 -25. doi:https://doi.org/10.1016/j.jnca.2021.103232

Sarra, C. (2022). *Il mondo-dato. Saggi sulla datificazione e diritto.* Cleup.

Schmitt, C. (1984). *Dottrina della costituzione.* Giuffré.

Schollmeier, R. (2001). A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. *Proceedings First International Conference on Peer-to-Peer Computing*, (p. 101-102). Linköping. doi:10.1109/P2P.2001.990434

Scianella, L. G. (2015). La "Digital Nation" e il futuro dello "Stato-nazione". Il caso di "eEstonia". *DPCE*, p. 9 - 34.

Sciannella, L. G. (2020, aprile - giugno). Il Remote Internet Voting in prospettiva comparata. Il caso dell'Estonia. *Diritto pubblico comparato ed europeo*(2), p. 451 - 476. doi:10.17394/97521

Shifferaw, Y., & Lemma, S. (July 2021). Limitations of Proof of Stake algorithm in blockchain. *Journal of EEA, 39*, 81 - 95.

Soud , M., Helgason, S., Hjálmtýsson, G., & Hamdaqa, M. (2020). TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts. *2nd Conference on Blockchain Research & Applications for Innovative Networks and Services*, (p. 176 - 183). Paris. doi:10.1109/BRAINS49436.2020.9223306

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti , H., MacAlpine, M., & Halderman, J. (novembre 2014). Security Analysis of the Estonian Internet Voting System., (p. 703-715). doi:https://doi.org/10.1145/2660267.2660315

Stančíková , I., & Homoliak, I. (2023). SBvote: Scalable Self-Tallying Blockchain-Based Voting. *Proceedings of the 38th ACM/SIGAPP Symposyum on Applied Computig. Association for Computing Machinery*, (p. 203- 211). New York. doi:https://doi.org/10.1145/3555776.3578603

Sun, J., Yan, J., & K. Zhang , K. (2016). Blockchain-based sharing services: what blockchain technology can contribute to smart cities. *Financial Innovation*, 2. doi:10.1186/s40854-016-0040-y

Sun, X., Yu, F., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021, July/August). A Survey on Zero-Knowledge Proof in Blockchain. *IEE Network, 35*(4), 198-205. doi:10.1109/MNET.011.2000473

Tanwar , S., Parekh , K., & Evans , R. (2019). Blockchain - based electronic healthcare record system for healthcare 4.0. applications. *Journal of Information and Security*, 2. doi:https://doi.org/10.1016/j.jisa.2019.102407

Tasmia Alvi , S., Nasir Uddin, M., Islam, L., & Ahame, S. (2022, July 1st). DVT Chain: a blockchain - based decentralized mechanism to ensure the security of digital voting system. *Journal of King Saud Univeristy, Computer and Information Sciences*, 6857 - 6871. doi:HTTPS://DOI.ORG/10.1016/J.JKSUCI.2022.06.014

Treiblmaier , H., Rejeb , A., & Strebinger , A. (2020). Blockchain as a Driver for Smart City Development: Application fields and Comprehensive Research Agenda. *Smart Cities*, 853-854. doi:10.3390/smartcities3030044

Tronconi, F. (2022, aprile - giugno). Il movimento 5 stelle in cerca di futuro . *Il Mulino*, 65 - 75. doi:10.1402/104126

Uddin, M. (2021, 4th January). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, 1-16. doi:https://doi.org/10.1016/j.ijpharm.2021.120235

Ul Abadin, Z., & Haider Syed , M. (7th July 2021). A Pattern for Proof ofWork Consensus Algorithm in Blockchain. *EuroPLoP '21.* Gratz.

Universale, la grande enciclopedia tematica. (2005). *Bulè, 17*, 200. Milano: Garzani libri S.p.A.

Universale, la grande enciclopedia tematica. (2005). *Ecclesia, 17, 441*. Milano: Garzani libri S.p.A.

Universale, la grande enciclopedia tematica. (2005). *Solone, 18*, 1332 . Milano, Italia: Garzanti libri S.p.A.

Vedel, T. (2006). The Idea of Electronic Democracy: Origins, Visions and Questions. *Parliamentary Affairs, 59*(2), 226 - 230. doi:10.1093/pa/gsl005

World Health Organization. (2018). *mHealth: Use of appropriate digital technologies for public health.* Tratto da https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_20-en.pdf

Xiong , H., Chen, M., Wu, C., Zhao, Y., & Yi, W. (2022). Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms. *Future Internet, 14*(47). doi:https://doi.org/10.3390/fi14020047

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview.* doi:https://doi.org/10.6028/NIST.IR.8202

Zhou, Q., Huang , H., Zheng , Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. *IEEE Access, 8*, 16440 - 16455. doi:10.1109/ACCESS.2020.2967218

Sitografia

https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/blockproposal/

https://btcscan.org/

https://101blockchains.com/delegated-proof-of-stake-dpos/

1*https://101blockchains.com/crypto-wallets/*. Tratto da https://101blockchains.com/crypto-wallets/

Agenda digitale. Tratto da Che cosa sono i cookies : https://www.agendadigitale.eu/infrastrutture/tutto-quello-che-dobbiamo-sapere-sui-cookie-per-la-privacy-da-utenti-o-gestori/

https://auraconsortium.com/about

https://auraconsortium.com/customer-journey

Barlow, J. P. (1996). *Electronic Frontier Foundation*. Tratto da https://www.eff.org/it/cyberspace-independence

Benaloh, J. (2006, June 14th). Simple Verifiabile Elections. Tratto da https://home.ipipan.waw.pl/w.jamroga/papers/benalohGT23evote-final-arxiv.pdf

BSI (2017) Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. *Overview Report*. Tratto da https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf

Camera. *Proposta di disegno di legge costituzionale n.2816/2015*. Tratto da http://documenti.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0028730.pdf

Camera. *Proposta di disegno legge costituzionale n.327/2022*. Tratto da http://documenti.camera.it/leg19/pdl/pdf/leg.19.pdl.camera.327.19PDL0008910.pdf

CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies (FG - BDLT). (2018, September 20th). Reccomendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger / Bloccckhain Technologies. 9 - 87. Tratto da https://www.cencenelec.eu/media/CEN-CENELEC/Areas%20of%20Work/CEN%20sectors/Digital%20Society/Emerging%20technologies/fg-bdlt-white_paper-version1-2.pdf

https://www.chronicled.com/about-us

Commissione delle comunità europee. (2003, settembre 26). Il ruolo dell'eGovernment per il futuro dell'Europa. *COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO, AL PARLAMENTO EUROPEO, AL COMITATO ECONOMICO E SOCIALE*. Bruxelles. Tratto da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52003DC0567

Commissione per i diritti e i doveri relativi ad Internet. (2015). *Camera.it*. Tratto da https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

Consiglio d'Europa. (1950). CEDU. Tratto da https://rm.coe.int/1680063777

Crouch, C. (2004). Riflessioni sulla postdemocrazia. *La Società degli individui*, 3 - 4 . Tratto da https://pure.mpg.de/rest/items/item_1234167_3/component/file_1854704/content

Dai, W. (1998). Tratto da http://www.weidai.com/bmoney.txt

Decreto 8 aprile 2024 - Concorso per esami a 400 posti di magistrato ordinario. (s.d.). Tratto da https://www.giustizia.it/giustizia/it/mg_1_8_1.page?contentId=SDC467378

EBA. (2014, July 4). EBA Opinion on 'virtual currencies'. Tratto da https://www.bancaditalia.it/compiti/sispaga-mercati/strumenti-pagamento/normativa/EBA-Op-2014-08-Opinion-on-Virtual-Currencies.pdf

Enciclopedia Treccani. (s.d.). *Voce consorzio*. Tratto da https://www.treccani.it/vocabolario/consorzio/

Enciclopedia Treccani. (s.d.). *Voce dittatore*. Tratto da https://www.treccani.it/enciclopedia/dittatore_(Enciclopedia-Italiana)/

Enciclopedia Treccani. (s.d.). *Voce partecipazione elettorale*. Tratto da https://www.treccani.it/enciclopedia/partecipazione-politica_(Enciclopedia-delle-scienze-sociali)/

Enciclopedia Treccani. (s.d.). *Voce polarizzazione*. Tratto da https://www.treccani.it/vocabolario/polarizzazione/

Enciclopedia Treccani. (s.d.). *Voce Stato di diritto*. Tratto da https://www.treccani.it/enciclopedia/stato-di-diritto_(Dizionario-di-Storia)/

Europarl, Carta di Nizza. (2001). Tratto da https://www.europarl.europa.eu/charter/pdf/text_it.pdf

Github. (s.d.). Tratto da https://gist.github.com/chris-belcher/9144bd57a91c194e332fb5ca371d0964

Hoek , J., Dai , Y., Lai , E., & Zhang, T. (s.d.). Tratto da https://student.cs.uwaterloo.ca/~cs446/1171/Arch_Design_Activity/Peer2Peer.pdf

http://legislature.camera.it/_dati/costituente/lavori/iii_sottocommissione/sed009/sed009nc.pdf#page=4&zoom=95,0,70

https://101blockchains.com/federated-blockchain/

https://101blockchains.com/permissioned-blockchain/

https://academy.bit2me.com/it/que-es-coinjoin/

https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1. (s.d.). Tratto da https://csrc.nist.gov/news/2006/nist-comments-on-cryptanalytic-attacks-on-sha-1

https://digiexpo.e-estonia.com/story-of-e-estonia/

https://dlt.mobi/about/

https://dlt.mobi/mobi-announces-the-first-vehicle-identity-vid-standard-on-blockchain-in-collaboration-with-groupe-renault-ford-and-bmw-among-others/

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi

https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+ebsi#how-it-works

https://edition.cnn.com/2000/ALLPOLITICS/stories/11/15/jackson.punchcards/;https://supreme.justia.com/cases/federal/us/531/98/

https://e-estonia.com/story/

https://ethereum.org/it/roadmap/merge/issuance/#cl-issuance-post-merge

https://etherscan.io/txs

https://followmyvote.com/blockchain-voting-the-end-to-end-process/

https://help.instagram.com/581066165581870

https://it.kamiltaylan.blog/nonce/

https://legislature.camera.it/cost_reg_funz/667/1157/859/documentotesto.asp

https://medium.com/@jordans2299/revisiting-the-dao-hack-33224d641303

https://medium.com/geekculture/introduction-to-hyperledger-fabric-1ce0a1d67494

https://medium.com/techskill-brew/hash-functions-in-blockchain-part-3-blockchain-basics-c3a0286064b6

https://medium.com/thedarkside/how-bitcoin-works-everything-you-need-to-know-8442f0c8627f

https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government

https://scienzepolitiche.unical.it/bacheca/archivio/materiale/143/Storia%20contemporanea/Dichiarazione%20diritti%20uomo%20e%20cittadino%201789.pdf

https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168071bc84

https://sha256algorithm.com/

https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf

https://supreme.justia.com/cases/federal/us/531/98/

https://thecryptogateway.it/proof-of-stake/

https://transparency.meta.com/features/explaining-ranking/

https://ultrasound.money/

https://voatz.com/security-and-technology/

https://www.bitpanda.com/academy/it/lezioni/tutto-quello-che-devi-sapere-sugli-alberi-di-merkle/

https://www.britannica.com/money/Sean-Parker

https://www.coe.int/t/dgap/goodgovernance/Activities/Key-Texts/Recommendations/00Rec(2004)11_rec_adopted_en.asp

https://www.educationestonia.org/tiger-leap/

https://www.encryptionconsulting.com/education-center/what-is sha/#:~:text=SHA%20stands%20for%20secure%20hashing,modular%20additions%2C%20and%20compression%20functions.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

https://www.eublockchainforum.eu/about

https://www.europarl.europa.eu/election-results-2019/it/affluenza/

https://www.gemini.com/it-it/cryptopedia/what-is-tokenization-definition-crypto-token#section-the-benefits-of-tokenization

https://www.geopop.it/bit-byte-megabyte-e-gigabyte-cosa-sono-e-che-differenza-ce-tra-queste-unita-di-misura-informatiche/

h https://www.hola-cripto.com/glossario-criptovalute/cypherpunk-significato/

https://www.ibm.com/it-it/topics/api

https://www.internazionale.it/bloc-notes/annalisa-camilli/2019/02/18/diciotti-matteo-salvini

https://www.interno.gov.it/it/notizie/quando-e-come-vota-elezionipolitiche2022

https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

HTTPS://WWW.MAKEUSEOF.COM/TAG/P2P-PEER-PEER-FILE-SHARING-WORKS/

https://www.medicitalia.it/chi-siamo/

da https://www.microsoft.com/it-it/security/business/security-101/what-is-a-ddos-attack

https://www.movimento5stelle.eu/votazione/

https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard

https://www.openpolis.it/lastensionismo-e-il-partito-del-non-voto/

https://www.penaledp.it/wp-content/uploads/2023/02/decisione-della-Suprema-Corte-di-Cassazione-di-Torino.pdf

https://www.repubblica.it/tecnologia/2021/06/15/news/skyvote_al_posto_di_rousseau_m5s_rassicura_i_dati_sono_al_sicuro-306162854/

https://www.riigiteataja.ee/en/eli/514122020002/consolide

https://www.salute.gov.it/portale/nuovocoronavirus/archivioFakeNewsNuovoCoronavirus.jsp.

https://www.saluteinternazionale.info/2016/07/big-pharma-una-storia-che-si-ripete/

https://www.tiot.it/smart-city/illuminazione-stradale-solo-dove-e-quando-serve/

HTTPS://WWW.WIRED.IT/PLAY/MUSICA/2014/06/03/LA-STORIA-DI-NAPSTER/

https://x.com/it/tos

Hughes, E. (1993). *A Cypherpunk's Manifesto*. Tratto da https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt

https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/HL_Whitepaper_IntroductiontoHyperledger.pdf

Il sole 24 ore. Tratto da https://www.ilsole24ore.com/art/nel-2023-11930-attacchi-cyber-7percento-diramati-oltre-75mila-alert-AFzxSuCC

Kaspersky Lab. Tratto da https://gsma.my.site.com/mwcoem/servlet/servlet.FileDownload?file=00P690000308eNaEAI

May, T. (1992). *The Crypto Anarchist Manifesto*. Tratto da https://activism.net/cypherpunk/crypto-anarchy.html

Medicalchain. (2018). Medicalchain Whitepaper. Tratto da https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

Menietti, E. (2018, marzo 19). *Il caso Cambridge Analytica spiegato bene*. Tratto da Il post: https://www.ilpost.it/2018/03/19/facebook-cambridge-analytica/

Ministro per le riforme istituzionali e la semplificazione normativa. *Riforma sul taglio dei parlamentari*. Tratto da https://www.riformeistituzionali.gov.it/it/la-riduzione-del-numero-dei-parlamentari/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Chash System. 1-9. Tratto da https://bitcoin.org/bitcoin.pdf

National Geographic. Tratto da https://www.storicang.it/a/nascita-della-polis-trasforma-grecia_15848

Norman, J. (s.d.). *History of information*. Tratto da https://www.historyofinformation.com/detail.php?id=3411

OECD. (s.d.). *Open Government*. Tratto da https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/Racc_Consiglio_sul_Governo_Aperto.pdf

Pagella politica . *Spesa istituzioni*. Tratto da https://pagellapolitica.it/articoli/costi-politica-parlamento-governo-ministeri

Pariser, E. (s.d.). *Ted Talk* . Tratto da YouTube: HTTPS://WWW.YOUTUBE.COM/WATCH?V=B8OFWFX525S

Parlamento Europeo. *Definizione di big data* . Tratto da https://www.europarl.europa.eu/topics/it/article/20210211STO97614/big-data-definizione-benefici-e-sfide-infografica

Rai . Tratto da https://www.rainews.it/video/2022/09/il-video-di-giorgia-con-due-meloni-alla-vigilia-del-voto-d56bb707-b6db-4bca-a503-a2fee5ae270e.html

Rivest, R. (1992, April). The MD5 Message - Digest Algorithm. Tratto da https://www.ietf.org/rfc/rfc1321.txt

Senato. *Proposta di disegno di legge costituzionale n.2485/2010*. Tratto da https://www.senato.it/service/PDF/PDFServer/BGT/00519114.pdf

Sky Tg24.Tratto da https://tg24.sky.it/cronaca/approfondimenti/tangentopoli-protagonisti-mani-pulite#04

Smart contract, Szabo. (1994). Tratto da https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

https://thecryptogateway.it/proof-of-stake/

UNESCO . *Definizione di e-governance*. Tratto da https://webarchive.unesco.org/20161021003528/http:/portal.unesco.org/ci/en/ev.php-URL_ID=4404&URL_DO=DO_TOPIC&URL_SECTION=201.html

United Nations. *Definizione di diritti umani*. Tratto da https://www.ohchr.org/en/what-are-human-rights

United Nations. *Definizione di e-government*. Tratto da https://publicadministration.un.org/egovkb/en-us/Overview

Villaschi, P. (2020, marzo 20). Voto e partecipazione nel sistema "Rousseau": di quale democrazia stiamo parlando? *AIC, Associazione italiana dei costituzionalisti* (1), 589 - 615. Tratto da https://www.rivistaaic.it/images/rivista/pdf/1_2020_Villaschi.pdf

World Bank. *Definizione di e-government*. Tratto da https://www.worldbank.org/en/topic/digitaldevelopment/brief/e-government

www.rousseau.movimento5stelle.it . Tratto da www.rousseau.movimento5stelle.it