El voto a través de internet mediante tecnología *blockchain*

Online voting through blockchain technology

MARIO GIL LLORIA
Estudiante del Máster Universitario de Derechos Humanos, Democracia y Justicia Internacional Universitat de València
gilloma@alumni.uv.es

DOI: https://doi.org/10.7203/cc.5.30242

Fecha de recepción: 17/06/2024
Fecha de aceptación: 30/11/2024

Resumen
El trabajo trata de una aproximación a la institución del voto como elemento de resolución de conflictos políticos en los estados democráticos, a través del estudio de las distintas metodologías que existen a la hora de emitir el sufragio, con especial referencia al voto a través de Internet. Esto permite poner de manifiesto tanto las ventajas que este método aporta frente a los sistemas de emisión del sufragio analógicos y electrónicos presenciales, como los problemas que plantea la implementación de un sistema de voto electrónico remoto a través de Internet, especialmente en lo que a la seguridad respecta. Ante estas dudas, la tecnología *Blockchain* se presenta como una alternativa para asegurar el anonimato y el sentido del voto frente a actores internos y externos al sistema, de modo que las máximas reticencias de este modo de sufragio podrían quedar solventadas.

Palabras Clave
Derecho de sufragio; voto electrónico; voto *online*; seguridad, tecnología *Blockchain*.

Abstract
The work deals with an approach to the institution of voting as an element of political conflict resolution in democratic States, through the study of the different methodologies that exist when casting the vote, with special reference to voting via the Internet. This makes it possible to highlight both the advantages of this method compared to analogical and face-to-face electronic voting systems, as well as the problems posed by the implementation of a remote electronic voting system via the Internet, especially in terms of security. Given these doubts, Blockchain technology is presented as an alternative to ensure the anonymity and the sense of the vote against internal and external actors to the system, thus, the greatest reluctance of this method of voting could be solved.

Keywords
Voting rights; electronic voting; online voting; security; Blockchain technology.

Sumario

Cuadernos Constitucionales 5, pp. 97-102

I. Introducción

Como es sabido, el voto es una de las principales herramientas que se utilizan para dirimir las cuestiones que se plantean en el seno de una sociedad compleja. Se configura, en el plano teórico, como un derecho fundamental de especial protección en los sistemas legales y, desde un punto de vista pragmático, es el principal mecanismo por el que la ciudadanía puede expresar de manera pacífica sus posiciones políticas, bien sobre una cuestión concreta (referéndums y plebiscitos), bien para la elección de representantes políticos.

El voto constituye una herramienta de democratización e igualación de los ciudadanos. De acuerdo con Mill (1878: 191) no existirá la igualdad en el sufragio cuando el voto de cualquier individuo sea de distinto valor.

En esta línea, Rebato Peño (1998:228) expone que uno de los ejes fundamentales del estado democrático es la participación ciudadana en los asuntos públicos, sea en su vertiente de elegible, sea en la de elector, es decir, mediante el ejercicio de su derecho a voto. Es más, el TC se ha pronunciado en reiteradas ocasiones en este sentido (entre otras, SSTC 26/1990 de 19 de febrero-FJ 3º- y 27/1990 de 22 de febrero), caracterizando el derecho a sufragio activo como elemento central de un sistema democrático, incluso calificándolo como la "piedra angular del sistema democrático".

Dada la importancia que tiene el voto, el método de emisión es un factor relevante y debe generar confianza plena en la ciudadanía. Es necesario que el sistema garantice que no se va a modificar el sentido del voto y que, con toda seguridad, se va a respetar el secreto de la opción política de quien lo emite. Ello ha llevado a consolidar a lo largo de los dos últimos siglos un sistema de voto que preserve el anonimato y el sentido del voto emitido.

El avance tecnológico abre un mundo de posibilidades para el ejercicio del derecho de sufragio. Los sistemas de voto analógico pueden comenzar a ser sustituidos por voto electrónico, introduciendo elementos digitales dentro del proceso de votación, que van desde la emisión hasta el recuento final, lo que da lugar a la aparición de diferentes niveles de complejidad en el voto electrónico.

Entre las distintas clases de voto electrónico que se llevan desarrollando desde hace más de tres décadas, surgen nuevas posibilidades, como es la de implementar el voto *online*, es decir, la emisión del voto de manera telemática a través de Internet.

Hay diferentes modos de configurar el voto *online*, pero todos ellos encuentran lagunas en lo que a la seguridad respecta. Para remediar estas dudas, en el

ISSN: 2660-9231

presente trabajo presento la tecnología *Blockchain* como una alternativa viable en términos de seguridad.

En mi opinión, mediante esta tecnología es posible aportar un nivel de seguridad superior, incluso, al de los modelos de voto tradicional, pues se pasa de depositar la confianza en los individuos que conforman el sistema de votación a que esta recaiga en un sistema algorítmico y neutro ideológicamente. Asimismo, expondré la proyección de esta tecnología en el ámbito del derecho electoral, constatando su viabilidad.

La finalidad es, pues, realizar un estudio de aproximación a un tema complejo y necesitado de análisis (la bibliografía específica es prácticamente inexistente), para intentar comprender el sentido del voto en una sociedad democrática, donde la elección se concibe como un derecho fundamental, lo que lo caracteriza como uno de los ejes nodales de los estudios del constitucionalismo.

II. El voto y sus metodologías

Antes de entrar a valorar los riesgos y las ventajas del voto *online,* resulta conveniente contextualizar las formas en las que los ciudadanos pueden expresar su voluntad política y los elementos esenciales que deben adornar al proceso desde un punto de vista democrático, para así explicar las carencias y las virtudes de la propuesta que se expone.

Es común advertir que el derecho de sufragio tiene dos vertientes: la pasiva, esto es la capacidad de ser elegido como representante, y la activa, que constituye la capacidad de elegir al representante. Esta última conforma el eje central del derecho al voto.

El derecho al voto es un derecho subjetivo que, como señala Presno Linera (2011:11), representa una facultad jurídica otorgada por la Constitución a un individuo para que este pueda ejercer, proteger o garantizar ciertas expectativas de participación política. Este derecho depende de condiciones subjetivas diversas, entre las que destacan "la universalidad del sufragio, la libertad de voto y la igualdad de trato entre los electores" (Pérez Alberdi, 2013:345). Gracias a la fuerza normativa de la Constitución, dicha facultad implica la posibilidad de exigir a los poderes públicos que garanticen la participación, ya sea de forma directa o a través de representantes, en la gestión política de la comunidad.

Los sujetos facultados para participar se fijan legislativamente por el estado. En una democracia el sistema es de sufragio universal, en el que los límites al derecho son mininos. Históricamente no ha sido así, pues el derecho al voto no era igualitario, y las excepciones obedecían a razones discriminatorias como el sexo, la clase social, el rol familiar o los motivos raciales, vulnerando de este modo el principio de igualdad[1].

Cuando el sufragio activo se ejerce, debe someterse a los filtros de cada sistema electoral, donde el voto ciudadano se transforma, bien en la elección de los representantes, que ejercerán el poder político o bien refrendando una decisión política concreta.

El voto tiene una doble proyección objetiva/subjetiva, cuyos requisitos esenciales e irrenunciables son cuatro: sufragio universal, libre y secreto, igual y directo y personal.

1 Ejemplos son el reconocimiento del derecho a voto femenino en Suiza que no se alcanzó hasta el año 1971, o el reconocimiento del voto a personas no blancas en Sudáfrica en 1994.

Cuadernos Constitucionales 5, pp. 97-102

La universalidad supone que, en la organización de los procesos electorales, no se considerará ninguna circunstancia de índole personal, social, cultural, económica o política para determinar quién tiene derecho al sufragio (Presno Linera, 2016: 280-281).

Este no es un derecho absoluto. Los estados han de establecer unas condiciones mínimas para poder ejercerlo, pero no han de ser contrarias a sus características intrínsecas. En este sentido, el TEDH en el caso Hirst v. the United Kingdom nº 2 se pronuncia defendiendo que *es posible que, en los estados democráticos contemporáneos, exista una presunción de sufragio universal. Sin embargo, esto no significa que el estado no pueda restringir el derecho al voto, a elegir y a postularse para elecciones*[2].

El requisito de voto libre y secreto resulta imprescindible para entender la problemática que se pretende analizar. En caso de que el ciudadano que ejerce su derecho a voto se encuentre bajo cualquier tipo de coacción o amenaza el proceso no será verdaderamente democrático ya que se votará según la convicción de un tercero y no según la propia voluntad; de esta premisa se deriva que el voto sea secreto (Presno Linera, 2016: 289), para lo que existen una serie de requisitos de seguridad que cualquier sistema democrático deberá respetar.

Por su parte, el sufragio igual consiste en atribuir idéntico valor a los votos emitidos, como consecuencia del principio de igualdad formal, sin discriminar de esta manera opiniones o posiciones políticas, ya que en el seno de un estado democrático se tiene al pluralismo político como uno de los valores superiores. Esta premisa se cumple garantizando que cada ciudadano disponga de la misma cantidad de votos o papeletas.

En último lugar, el sufragio debe ser directo y personal, esto es, los electores deben elegir por ellos mismos y no por medio de terceros, a sus representantes.

Cabe señalar que, además de ser considerado un derecho fundamental, debe cumplir una serie de premisas jurídico-formales, que establezcan claramente cómo se desarrollarán los procesos electorales.

En el momento actual, la mayoría de sistemas electorales son analógicos y se estructuran mediante la emisión presencial del voto a través de papeletas físicas, lo que no encierra ninguna complejidad, ya que es la metodología empleada desde el inicio de los sistemas democráticos y es de sobra conocida.

No digo nada nuevo si sostengo que la irrupción de las tecnologías ha invadido todos los ámbitos de la vida: la cultura, la política, la economía, etc., produciendo grandes cambios en las sociedades modernas. España no es la excepción y la Administración ha llevado a cabo un proceso de digitalización en casi todos sus ámbitos lo que ha permitido introducir mecanismos de emisión electrónica del voto (Presno Linera, 2016: 279).

Según explica Criado el desarrollo de administración digital se centró en primer lugar en el desarrollo de servicios públicos digitales, pero a partir de la segunda década del siglo XXI, se comienzan a introducir los servicios digitales en las tareas de gobernanza, lo que lleva a reconducir la administración digital a tareas de transparencia, participación ciudadana y colaboración e innovación pública. De esta manera comienzan los servicios de gobierno abierto y administración electrónica sumado a la idea de administración totalmente digital (Criado, 2021: 77).

Todo este avance lleva a pensar que la administración electoral, pase a vivir una suerte de reconversión hacia la administración electrónica, incluso en el acto

2 Texto original. "There may well be, in contemporary democratic States, a presumption of universal suffrage. This does not mean, however, that the State is unable to restrict the right to vote, to elect and to stand for election".

ISSN: 2660-9231

de votación, lo que lleva a pensar a una parte de la doctrina, con la que estoy de acuerdo, que los sistemas de votación analógico acabarán desapareciendo (Cano, 2000: 64-65 y Gálvez Muñoz, 2009: 262).

Pero, en el momento actual, entiendo que todavía hay que ser precavido con el uso de sistemas electrónicos para emitir el voto, ya que se desconoce el impacto real que pueda llegar a tener. Por esto, autores como González De La Garza (2009: 235) se posicionan en contra de esta modalidad, afirmando que el sistema de voto electrónico (presencial y remoto mediante Internet) no se compadece con las exigencias de confiabilidad suficientes por lo que generan inseguridad y no aportar ventajas significativas en ningún sentido relevante.

Ante estas posiciones, y el tradicional retraso de la Administración en adecuarse a las novedades, es posible afirmar que la administración electoral de nuestro entorno no se ha modernizado, tal y como también afirma la doctrina mayoritaria, lo que seguramente tiene que ver, como afirma Martínez Dalmau (2013: 140), con la falta de obligatoriedad de instaurar sistemas electrónicos en el ámbito electoral en la mayoría de los países europeos.

En España se ha legislado en materia de voto electrónico únicamente en el País Vasco. Es la Ley 15/1998, de 19 de junio, de modificación de la Ley 5/1990, de 15 de junio, de Elecciones al Parlamento Vasco, la que alude a la introducción de un sistema de voto electrónico, que a día de hoy, y pese a la modificación de la norma, no ha sido todavía implementado en ninguno de los procesos electorales del Parlamento vasco, donde se mantiene el sistema tradicional de voto a través de papeletas, pudiéndose ejercer el derecho a voto de manera presencial o a través del mecanismo del voto por correo (Fernández Riviera, 2001: 213-214).

La falta de legislación es uno de los motivos de la dificultad para implementar los sistemas de voto electrónico, sea en su vertiente presencial, sea a través de Internet, sistema que todavía no cuenta con una gran implantación, ni desarrollo. Es cierto que tampoco es obligatorio digitalizar en otros ámbitos de la Administración donde sí se ha introducido la *e-administration*, lo que me lleva a reflexionar sobre cuál es la razón añadida para que no se haya producido el cambio en el ámbito electoral. Quizá, dificultades técnicas y económicas para el desarrollo del ejercicio del derecho con todas las garantías sea el motivo de mayor peso para ello

III. El voto electrónico

La necesidad de digitalizar la administración electoral es cada vez más patente, pues facilita la expresión de la voluntad ciudadana y hace más transparente el ejercicio del derecho al sufragio lo que permite alcanzar una mayor calidad democrática.

Según Gálvez Muñoz (2009:262), es inevitable la implementación del voto electrónico como metodología de uso general, es una cuestión de tiempo, pero se desconoce cómo y cuándo se puede producir el cambio pues las modalidades y ritmos de introducción de las metodologías de voto electrónico son muy variados. Con este punto de partida, se puede decir que el voto electrónico consiste en emitir la decisión en la que consiste el voto a través de medios electrónicos, tales como una urna electrónica o un ordenador sumado a un entramado tecnológico que permite que tanto el ejercicio del voto como su escrutinio, garantizando el registro y control de la identidad, el recuento de los sufragios, la transmisión de los resultados y la asignación de los puestos a elegir. (En este sentido Presno Linera, 2011: 104 y Fernández Rodríguez, 2007: 2010).

Cuadernos Constitucionales 5, pp. 97-102

Dentro del voto electrónico podemos encontrar distintas clases, pero, antes de pasar a analizar cada una de ellas, creo que conviene clasificar los tres niveles de automatización de las tareas dentro de los sistemas de *e-voting*. En este sentido, la doctrina habla de tres niveles (Gómez Oliva y Pérez Belleboni 2014: 35-36):

El nivel básico de automatización se refiere a aquellos supuestos de ejercicio analógico del derecho al voto (a través de papeletas), pero donde ya existen algunas fases complementarias del procedimiento automatizadas a través de herramientas informáticas y telemáticas. Por ejemplo, el registro de votantes, la generación y publicación del censo electoral o las actas de recuento final de votos. Al ser un sistema en el que la emisión del voto es analógica, hay que reflexionar hasta qué punto estaríamos ante un primer ejercicio de votación electrónica. En mi opinión, no podemos entender esto como la primera forma de voto electrónico, pero sí un acercamiento al mismo y a la aplicación de los mecanismos tecnológicos y, por lo tanto, un paso a una primera digitalización del sufragio.

El siguiente nivel, es el intermedio. En este, la emisión del voto sí se produce ya por medios electrónicos, por lo que ya estamos ante un verdadero sistema de votación electrónica, donde el votante ya ha sido previamente identificado y autentificado por este mecanismo. Además de la emisión del voto por medios electrónicos, también el recuento de votos, la generación de actas y, si procede, la publicación de resultados está digitalizado. La metodología empleada en este nivel consiste en la sustitución de las urnas por máquinas que se encargan de registrar y archivar los votos emitidos e, incluso pueden llegar a generar algún tipo de justificante. También el escrutinio y la redacción del acta final se produce de manera digital.

Por último, el nivel avanzado es aquel en el que la votación se hace de manera telemática. En este modelo se emplea la tecnología para la identificación y la autentificación del ciudadano. A partir de ahí, se procede a autorizar el ejercicio del derecho, autorización que se transmite con cumplimiento de todos los requisitos de seguridad, eliminando en el proceso cualquier momento analógico en la relación ciudadano-administración electoral. Un ejemplo del nivel avanzado es el voto *online,* donde todo el procedimiento se lleva a cabo electrónicamente.

El voto *online* se presenta como una modalidad de voto electrónico en la que la votación se realiza a través de Internet desde cualquier ubicación, de tal manera que la emisión del sufragio se dé fuera de los entornos típicos (véase los colegios electorales), y se envíe a través de un dispositivo con conexión a Internet no especializado en estas funciones. Una vez emitido el sufragio el sistema se encargaría de procesar la entrada del voto, registrarlo, transmitirlo a los servidores y publicar los resultados (Pascual Ginard, 2021: 14).

Evidentemente, los niveles de integración del voto electrónico en los sistemas electorales va a depender de las condiciones y circunstancias de cada Estado, lo que puede dar lugar a tres grupos de circunstancias, en atención al modo en qué físicamente se emite el voto: los casos en los que se decida incluir la modalidad electrónica como una posibilidad frente al voto tradicional en atención a los deseos del elector; hacerlo de modo complementario, esto es, permitiendo votar a través de un sistema mecánico que proporciona una papeleta que ha de introducirse de manera analógica en una urna al modo clásico, o lo que sería la transformación total con un sistema absolutamente tecnológico, dejando de lado las formas tradicionales (Gálvez Muñoz, 2009: 262-263).

También se pueden agrupar los requisitos para el desarrollo de una metodología de voto *online* en cinco categorías, tomando en consideración otros criterios como la seguridad o fiabilidad técnica, la garantía de los principios

ISSN: 2660-9231

básicos del sufragio, la integración armónica en el régimen electoral, el consenso o aceptación por parte de los implicados y la limitación de costes (Gálvez Muñoz, 2009:262).

Indudablemente la metodología de voto por Internet aporta gran cantidad de beneficios para una sociedad democrática, a pesar de la existencia de inconvenientes.

Para comenzar con las ventajas, hay que hablar de la mejora que genera en la gobernanza este sistema de votación, pues favorece la efectividad y la transparencia, que conforman los pilares básicos del *e-government* (Arroyo Chacón, 2017; Pascual Ginard, 2021: 24).

Del mismo modo aporta ventajas en el ámbito social, puesto que, según afirma Pascual Ginard el proceso se simplifica por la deslocalización que proporciona el Ciberespacio. Esto ayuda al ejercicio del derecho por parte de los más jóvenes, en la medida en que no tienen que desplazarse. Esta metodología igualmente soluciona el problema de determinados colectivos en los que concurren circunstancias especiales, como, por ejemplo, personas con dificultades de movilidad, o que residen en lugares aislados, o que se encuentran fuera de su lugar de residencia en el momento de la votación. Además, cabe mencionar los beneficios económicos que representa la implementación del voto online.

Es cierto que la instauración de este sistema debe ser gradual y progresiva, lo que obliga a que coexistan los sistemas electrónicos con los de voto tradicional y, por lo tanto, se duplica el gasto, a lo que hay que sumar, además, los costes de desarrollo de los programas informáticos. Sin embargo, y aunque pueda parecer una desventaja en una primera aproximación, a largo plazo lleva a reducir los gastos que supone un proceso electoral en términos económicos (Pascual Ginard, 2021:25) y a mi entender, facilita una mayor sostenibilidad desde un punto de vista ecológico.

En todo caso, también debo poner de manifiesto los aspectos negativos. Desde el análisis de los inconvenientes se deben señalar la posible falta de confianza del ciudadano en el sistema, su eficiencia, la brecha y el analfabetismo digital, la adaptación del voto tecnológico a la idiosincrasia del sistema electoral del Estado concreto y, sobre todo, la seguridad en el ejercicio del voto.

Es por ello que, habida cuenta de la complejidad que entrañan este modo de emitir el voto de manera electrónico, creo que la implementación de estos ha de ser pausada, progresiva y adaptándose a los nuevos avances tecnológicos que van sucediéndose.

Precisamente, para comprobar si el sistema es válido y, por lo tanto, mitigar estos efectos nocivos, conviene que la implementación del sistema de voto electrónico se de en convivencia con el sistema de voto tradicional, tal y como se proponía en la clasificación expuesta más arriba, de manera que, comprobada la eficacia y validez del sistema tecnológico, acabe sustituyendo al analógico, poco a poco. Además, los sistemas de voto electrónico deben desarrollar su infraestructura, y además, como ya he dicho, se debe concienciar a la población respecto de su uso. Por eso considero que sería aconsejable que se fuera realizando pruebas dándose este en un momento inicial respecto de consultas menores, para así conseguir mitigar los efectos sociales negativos que pueden existir, vinculados a la brecha digital en todas sus vertientes (generacional, por razones de género, de clase, etc.).

Cuadernos Constitucionales 5, pp. 97-102

IV. Seguridad en el voto a través de internet

Los sistemas de voto *online*, igual que los sistemas de voto tradicional o los de voto electrónico presencial, deben cumplir unos requisitos mínimos de seguridad, ya que el sufragio es uno de los elementos centrales del sistema democrático. Por ello, el proceso electoral debe estar protegido y cumplir con las garantías de la elección en todas sus vertientes, siendo de especial interés para este estudio la seguridad a la hora de ejercer el derecho de sufragio, sin olvidar las garantías jurídicas (Fernández Rodríguez, 2007: 215-221).

Conforme a Morales Rocha (2009:121 y 122), los requisitos de seguridad mínimos que todo sistema de voto electrónico remoto debe cumplir tienen que ver con la salvaguarda de los aspectos esenciales del ejercicio del derecho, que se mencionan en los primeros epígrafes, y los cifra en legitimidad, privacidad, precisión, equidad, verificación individual y universal, incoercibilidad y robustez.

En cuanto a la *legitimidad,* no debe haber fallos en relación con los sujetos que pueden ejercer el derecho de sufragio activo; por lo tanto, si solo pueden participar en el proceso electoral los sujetos autorizados y que hayan sido incluidos por los administradores electorales dentro del sistema, el sistema debe garantizar la correcta identificación del ciudadano para asegurar que el voto esté siendo ejercido por el titular del derecho y que no se falsea la identidad de este.

Como ya he ha afirmado, también resulta esencial garantizar el derecho al *secreto del voto,* por lo que el sistema debe asegurar la estricta separación entre la identidad del votante y el sentido de su voto, para mantener la privacidad.

La *precisión* exige que solo se tengan en cuenta los votos válidamente emitidos, debiendo ser excluidos del escrutinio los votos no válidos o duplicados, de tal modo que habrá que establecer unas reglas de revisión lo suficientemente seguras respecto de la identificación de aquellos votos que no deban ser contabilizados.

Por su parte, la *equidad* implica que no deben conocerse resultados parciales en la fase de votación, para evitar que estos influyan en el resultado global de las elecciones. Lo que supone dotar al sistema de las garantías suficientes para evitar que nadie pueda acceder a los resultados en el tiempo que transcurre la votación.

La *verificación individual* implica que cada votante pueda constatar que su voto ha sido correctamente recibido en el servidor y correctamente incluido en el escrutinio, para evitar fallos por cuestiones técnicas. Creo que esta garantía debería acompañarse de la posibilidad de rectificación, para el caso que se produzca el fallo.

En cuanto a la *verificación universal* es preciso dotar de mayor fiabilidad al sistema, permitiendo que cualquier persona, sea participante u observador, pueda comprobar la integridad de los resultados, lo que supone un plus de garantía respecto del voto presencial al permitir el acceso a un mayor número de observadores y una mayor muestra que si solo se puede estar presente, físicamente, en un recuento.

La exigencia de *incoercibilidad* significa que un votante no debe tener la posibilidad de demostrar a un tercero qué opción ha votado. Es decir, que el voto ha de ser absolutamente secreto sin posibilidad de prueba electrónica de cuál ha sido el sentido de este. Así se pueden reducir situaciones delictivas como coacciones o venta de voto, puesto que no se puede obtener validación de lo votado.

Además, la *robustez* del sistema es imprescindible, pues es lo que permite rechazar y evitar las amenazas que para la seguridad del proceso puedan proceder tanto desde el ámbito interno (fallos del sistema) como externo (ataques al sistema). Si existe el mínimo riesgo de una caída o fallo de seguridad en alguno de los aspectos expuestos, el sistema resulta inútil a los fines propuestos.

ISSN: 2660-9231

Evidentemente, todos los sistemas son susceptibles de ataques; ataques que tratarán de explotar alguna vulnerabilidad del procedimiento utilizado. Como he comentado más arriba, se trata de proporcionar el mayor nivel de seguridad posible, pero siempre pueden existir partes del sistema que sean menos seguras. Estas partes más vulnerables deben ser tenidas en cuenta a la hora de diseñar los procesos de voto electrónico remoto a través de Internet, para tratar de evitar al máximo su presencia y minimizar las consecuencias negativas, sin olvidar que en caso de que alguna de esas vulnerabilidades suponga un riesgo para los requisitos esenciales expuestos, deberán ser eliminadas o, en su caso, invalidarán el sistema. Morales Rocha (2009: 44-46) ofrece una serie de ejemplos de vulnerabilidades de las que puede adolecer un sistema de voto *online*, que se pueden resumir del siguiente modo:

En primer lugar, la posibilidad de encontrar un deficiente sistema de registro de votantes: tiene que ver con la correcta formación del censo electoral. Si los datos son erróneos, como también ocurre en ocasiones en los sistemas de votos tradicionales (por ejemplo, no inclusión de un ciudadano en el mismo) no se podrá garantizar el ejercicio legítimo del derecho a todos los ciudadanos.

En segundo lugar, pueden existir vulnerabilidades con un deficiente diseño de los mecanismos criptográficos empleados. Este aspecto se relaciona con el derecho a la intimidad de la opción votada. Si el mecanismo criptográfico resulta deficiente, los datos que deberían quedar encriptados podrían descifrarse, con riesgo de lesión de la privacidad de los usuarios.

En tercer lugar, puede darse un proceso de autenticación débil. Un sistema de voto *online* debe llevar aparejado un proceso de autenticación robusto para, de esta forma, evitar que se dé una suplantación de identidad que derive en una alteración de los resultados y viole el derecho del votante legítimo a ejercer o no su voto y en qué términos.

En cuarto lugar, una vulnerabilidad sería la existencia de terminales de votación inseguros. En la medida en que el voto se emite desde terminales particulares, no controlados por la administración electoral, existe la probabilidad de que adolezcan de algún problema de seguridad que pueda ser aprovechado por un potencial atacante. Por ello, considero que sería importante que para poder ejercer el derecho al voto de manera remota, la administración exigiera unos requisitos mínimos de seguridad, que se podrían implementar a través de la descarga obligatoria y gratuita de algún tipo de sistema de cortafuegos. Igualmente, debería habilitar puestos informáticos para que todas las personas que lo desearan pudieran ejercer el voto *online*, minimizando al máximo los problemas de brecha digital y de seguridad, al tratarse de puestos informáticos verificados por la propia administración.

En quinto lugar, los canales de comunicación inseguros son un problema, al igual que se ha afirmado en relación con los terminales, los canales de tránsito de la información deben ser seguros para evitar manipulaciones en el sentido del voto emitido, lo que pueden afectar a la elección.

En sexto lugar, pueden darse sistema de *logs* deficiente[3]: un registro inseguro de las transacciones llevadas a cabo en la elección produce una mayor probabilidad de ataques sin detección.

3 Por "log" se entiende la grabación secuencial de la información que afecta a un proceso particular quedando registrados todos los movimientos dentro de una base de datos. Ello es utilizado para constituir evidencia de los movimientos llevados a cabo dentro de un procedimiento.

Cuadernos Constitucionales 5, pp. 97-102

En séptimo lugar, también pueden sucederse procesos deficientes en la verificación de elementos. Durante el proceso de elección se deben llevar a cabo ciertos procesos de verificación, para determinar la correcta configuración y operación de los elementos que participan en la elección, pues su deficiencia puede producir una situación de vulnerabilidad.

Así pues, los sistemas de voto electrónico remoto a través de Internet pueden ser atacados a través de alguna de estas vulnerabilidades. Estas amenazas pueden venir tanto de elementos internos del sistema (los propios votantes y elementos de la administración electoral), como del exterior (elementos que no tienen relación directa con el proceso de elección). De nuevo es Morales Rocha (2009: 46-50) quien ofrece un catálogo de las distintas amenazas que, en su opinión, existen en los sistemas de voto electrónico remoto a través de Internet y que, en mi opinión, se pueden agrupar en tres tipos de amenazas.

El primer tipo de amenaza consiste en el proceso de autenticación puede ser alterado por situaciones tales como suplantación de identidad en el registro, manipulación del censo electoral, adquisición de credenciales de votante por quien no lo es, votar más de una vez, adición de votos ilegítimos, denegación del servicio a un ciudadano o grupo de ciudadanos, confabulación de la mesa electoral para alterar el resultado de la elección o violar la privacidad de los votantes o la captura de votos, sea para conocer el contenido o para modificarlo.

En segundo tipo de amenaza se da con la alteración de la voluntad del votante. Esta puede de dos formas: en primer lugar, mediante el uso de la fuerza bruta para obtener claves privadas de la elección (la clave privada es utilizada para descifrar los votos, por ello debe permanecer segura durante el proceso de elección) y la segunda amenaza consiste en la coerción y la compra de votos, para cambiar el sentido del voto que quisiera o no emitir el ciudadano.

El tercer tipo refiere al proceso. Este es susceptible de alteración mediante la manipulación del *software,* para atacar el sistema de registro, de configuración de la elección, de votación, o de consolidación de resultados entre otros. El daño al *hardware* implica la configuración errónea de la elección, manipulación del voto en el terminal de votación o sustitución de votos, que consiste en la alteración de los votos ya emitidos.

La verificación de cualquiera de estas amenazas conlleva un debilitamiento del sistema y una alteración del sentido democrático. Por ello, los sistemas de seguridad en el voto electrónico deben evolucionar hacia la neutralización de los riesgos para proporcionar un sistema lo más seguro posible. En todo caso, y junto a la formulación de una afirmación tan genérica y obvia, de futuro hay que analizar las posibilidades reales de que las mismas se produzcan y, por lo tanto, valorar el porcentaje de riesgo, ya que muchas de ellas no son distintas a las que se producen en el mundo *offline* y entran dentro de los márgenes de riesgo permitido por su baja incidencia.

V. La tecnología *blockchain* como una solución a los problemas de seguridad

Una vez analizado el problema de seguridad que acarrea el voto *online*, caben distintas soluciones para esta cuestión. De entre estas alternativas para favorecer la seguridad en el uso de mecanismos de voto a través de Internet destaca la tecnología *Blockchain*.

La tecnología *Blockchain*, en castellano "cadena de bloques", se define como "una tecnología del tipo de estructura de datos, que funciona como un libro mayor en el cual se registran transacciones que se almacenan dentro de bloques, dicho libro o cadena de bloques se almacena en todos los miembros

ISSN: 2660-9231

de la red, es decir, todos los miembros de la red guardan una copia del registro de las transacciones" (Lajpop Ajpacajá, 2021: 89).

De modo más sencillo se puede definir como "una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente (...) una base de datos descentralizada que no puede ser alterada" (Preukschat, 2017:23). Es fundamental que el sistema sea inalterable ya que, gracias a esta característica, la confianza de los usuarios puede ser plena en el sistema, pese a que exista desconfianza absoluta entre los usuarios.

La *Blockchain* se configura a partir de una red global de ordenadores que gestionan de manera autónoma los datos. Dentro de estas redes de ordenadores encontramos dos tipos principales de *Blockchain*. Por un lado, están las redes públicas en las que puede participar cualquier persona y, por otro lado, las redes privadas, que limitan el acceso a algunos participantes. En todo caso, estas redes sean públicas o privadas serán descentralizadas, es decir, no existirá una jerarquía o autoridad superior que verifique los procesos.

Conforme a Preukschat (2017:26 y 27) esta tecnología se compone de tres partes fundamentales: la criptografía, la cadena de bloques y el consenso. La combinación de los tres elementos en un *software* es lo que certifica la seguridad y fiabilidad de las operaciones realizadas en el marco de la tecnología *Blockchain*.

La *criptografía* es un procedimiento mediante el cual se transforma un mensaje cifrándolo y haciéndolo ininteligible para cualquier usuario que no tenga las claves adecuadas, que suelen ser personales. De esta forma, se busca asegurar que la información no sea manipulada, robada o se introduzca de manera deliberada información que no se corresponda con lo consensuado.

La *cadena de bloques* es la base de datos donde se almacena la información registrada por los usuarios de la red. Funciona de la siguiente manera: primero, se emite la información; seguidamente, esta es validada y se incorpora a un bloque, transmitiéndose al siguiente bloque y, gracias a la criptografía, esta información queda registrada en todos los bloques sin posibilidad de ser alterada.

El *consenso* se sustenta en el protocolo de verificación común, que permite comprobar las operaciones y asegura su inmutabilidad. Paralelamente, se aporta a todos los usuarios una copia inalterable y actualizada de las operaciones realizadas dentro de la red. Este proceso ya dota a la tecnología de una gran seguridad.

En esta línea, y conforme al estudio de Tapscott y Tapscott (2017: 56-88), cualquier tipo de red *Blockchain* debe cumplir con una serie de principios mínimos, que podrían resumirse en los siguientes:

El primero de todos es la integridad, consecuencia de la descentralización de la tecnología. Al no estar concentrada la información en un único nodo, esta debe encontrarse de manera íntegra en cada nodo.

Seguidamente encontramos el poder distribuido se deriva del carácter descentralizado de la *Blockchain*. El poder en este tipo de redes no se encuentra centralizado, ni jerarquizado. Todos los nodos tienen el mismo valor y jerarquía, o lo que es lo mismo, no existe un nodo central o dominante, ni tampoco una autoridad central que regule el modo de transitar, relacionarse o distribuir contenidos y datos por la red, tal y como afirman Alcántara Leiva (2011:33) y Miró Llinares (2012:155).

Por otro lado, la seguridad que proporciona la tecnología resulta de la distribución. Al estar la información recogida en todos los nodos y siendo que cada nodo no tiene acceso a toda la información, se consigue que los datos guardados estén protegidos con altos mecanismos criptográficos. Incluso, para

Cuadernos Constitucionales 5, pp. 97-102

modificar la información deberá emitirse una nueva transacción, quedando reflejados todos los cambios que se han sucedido, sin poder editarse ni borrarse, lo que permite el rastreo.

Además, se garantiza la *privacidad*, pues cada transacción está protegida hasta el punto de que únicamente puede acceder el dueño de la transacción haciendo uso de la contraseña que asignó. Por lo tanto, el conocimiento del contenido queda limitado a aquellos que poseen la contraseña.

La conjunción de estos principios configura la tecnología *Blockchain* que "está orientada a la privacidad, seguridad y transparencia de las transacciones" (Lajpop Ajpacajá, 2021: 90).

En definitiva, la *Blockchain* es cómo un libro electrónico en el que se contienen datos protegidos por una estructura matemática que lo hace inamovible.

La cuestión es si esta tecnología que se utiliza en transacciones económicas fundamentalmente, puede ser aplicación a un sistema de voto electrónico como modo de garantizar el anonimato y la veracidad del sentido del voto

En un primer momento la tecnología *Blockchain* únicamente servía para realizar transacciones económicas pero, progresivamente, conforme se ha investigado en la tecnología y sus usos, se han ido añadiendo distintas funcionalidades a la misma.

Dentro de estas distintas aplicaciones que encontramos en la *Blockchain*, podemos distinguir en tres tipos de tecnologías *Blockchain*, según la clasificación de Pérez Medina (2020:3), la *Blockchain* 1.0, que nació para la comercialización de las criptomonedas, la *Blockchain* 2.0 que se emplea en relación con los *Smartcontracts* y, por último, la *Blockchain* 3.0., que entiendo que puede tener aplicación en *e-Government*.

Conforme a Hjálmarsson y otros (2018: 984-985) la metodología consistiría en establecer un *smartcontract* para el voto electrónico, que se implementa dentro de la cadena de bloques, cumpliendo con los requisitos que debe asumir cualquier sistema de voto electrónico remoto. Para explicar el procedimiento lo dividiremos en dos bloques: la configuración de la *Blockchain* y el sistema de votación a través de los *smartcontracts*.

En primer lugar, hay que entender en qué consiste la configuración de la *Blockchain*. Para poder satisfacer los requisitos de seguridad, privacidad e independencia se debe contar con un espacio seguro a la hora de emitir el voto electrónico, para lo que se desarrolla un sistema basado esencialmente en dos tipos de nodos.

Así pues, encontramos en primer lugar, que a través de la *Blockchain* un nodo de distrito, en el que el administrador electoral crea una elección distribuyendo y desplegando un *smartcontract* para hacer constar la elección electoral. Cuando un votante individual emite su voto desde su *smartcontract*, los datos de su voto son verificados por los nodos de distrito correspondientes y cuando queda verificado, pasa a añadirse a la cadena de bloques.

Una segunda posibilidad es la que proporcionan los *Bootnode*, que consisten en un servicio de descubrimiento y coordinación para que los nodos del distrito puedan comunicar la información entre sí.

Respecto del sistema de votación a través de los *smartcontracts*, una vez ya se ha conformado una *Blockchain* segura y privada, adaptada para ejercer el voto *online*, el siguiente paso es desarrollar el *smartcontract* para que represente el proceso de votación electrónica y la decisión se transmita a la cadena de bloques.

Como ya he adelantado, es cierto que la mayoría de Estados no han introducido los sistemas de votación remota a través de Internet, principalmente porque la mayoría de la doctrina entiende que no gozan de toda la seguridad exigida. En este sentido, se afirma que que el principal desafío radica en el

ISSN: 2660-9231

riesgo de manipulación de las urnas o de las comunicaciones electrónicas, lo que puede derivar en una pérdida de confianza por parte de los ciudadanos en la integridad de los resultados electorales. Sin embargo, no es el único problema. También destacan otros como el riesgo de errores en la asignación de los votos, la posibilidad de un borrado accidental de los sufragios o las limitaciones tecnológicas que afectan a ciertos sectores de la población, especialmente los de mayor edad y los de menores recursos. Estos problemas se agravan en el caso del voto por Internet, debido a la falta de control directo sobre el acto de votar y a la necesidad de establecer una infraestructura de seguridad y comunicación más compleja y amplia (Ruiz González y Gálvez Muñoz, 2011:261).

Estas incertidumbres entiendo que pueden mitigarse con el sistema de voto *online* basado en tecnología *Blockchain* explicada. Gracias al tipo de criptografía utilizado y los múltiples sistemas de seguridad que lo complementan, la realización del voto a través de Internet utilizando la tecnología de cadena de bloques refuerza, en gran medida, los puntos vulnerables que se predican de otros sistemas de encriptado utilizados en procesos de voto electrónico, por lo que considero que su uso, puede ser la solución a las desconfianzas expuestas por la doctrina.

En este sentido, me parece muy interesante la explicación de Barrio Andrés (2022:102) cuando afirma que la tecnología *Blockchain* al descentralizar por completo el sistema proporciona una garantía de seguridad muy elevada, lo que se complementa con la posibilidad de rastreo cada vez que se realiza una nueva transacción lo que supone que el control del proceso pertenece a los usuarios y hace, prácticamente imposible, la alteración de la información contenida en los bloques. Esto aplicado a un sistema de voto electoral a través de Internet se traduce en eliminar en gran medida las dudas que se suscitan en torno a la seguridad ofrecida por las tecnologías que intervienen en el tratamiento de los datos en los procesos electorales.

Así pues, hasta el momento, la tecnología *Blockchain*, se presenta a mi modo de ver, como la mejor solución posible en una hipotética implementación de un sistema de voto electrónico remoto a través de Internet, debido a que es el formato que mayores garantías ofrece en los puntos que son fundamentales para calificar el sistema como democrático, pues es la tecnología que mejor garantiza tanto el anonimato (gracias a la imposibilidad de rastrear el voto) como la verificación del usuario.

En este sentido Llamas Covarrubias *et. al*. (2021) añaden que, junto a la implementación de este sistema debe configurarse una identidad digital de la ciudadanía que posteriormente derive en una auténtica ciudadanía digital. Para estos autores la ciudadanía digital consiste en el conjunto de derechos públicos y políticos de los ciudadanos, en virtud de los cuales se podría comprobar el consentimiento en los ámbitos digitales (derechos públicos) mientras que los derechos políticos supondrían la capacidad para poder ejercer derechos político-electorales.

Esto no quiere decir que esta tecnología no esté exenta de problemas, pues todavía se encuentra en un nivel de desarrollo menor que otras opciones centralizadas para este tipo de aplicaciones. Además, encuentra problemas en la autenticación de los votantes, que debe darse mediante una entidad centralizada, lo que abre la posibilidad a ataques informáticos (De Ávila, 2019:56), pues de momento, no se permite la descentralización absoluta.

Cuadernos Constitucionales 5, pp. 97-102

VI. Consideraciones finales

A la vista de lo expuesto creo que se pueden realizar las siguientes reflexiones:

En primer lugar, con la democratización del uso de las nuevas tecnologías e Internet, que destaca sobre todas ellas, la forma analógica tradicional de expresar las preferencias de la ciudadanía en una elección deja de ser la única opción viable. Estas tecnologías, sumadas al inevitable proceso de digitalización de las administraciones públicas, lleva a plantear que es una cuestión de tiempo que la tecnología se implemente en el marco de la administración electoral.

Ciertamente, y cómo he ido relatando, el proceso de digitalización del voto trae distintos problemas que deben ser abordados (la brecha digital íntimamente vinculada a la universalidad del sufragio; la eficiencia del sistema, las nuevas garantías y controles que deben aplicarse; la cuestión de adaptarse a la idiosincrasia de cada sistema electoral). En concreto, y en relación con el voto *online*, se plantean ciertas cuestiones particulares como son, la posible falta de confianza en el sistema, la alfabetización digital de los usuarios y el procedimiento interno de seguridad que proponga en su caso cada modelo, para mantener el anonimato del votante y la integridad de su voto.

Mas allá del uso de la tecnología *Blockchain* propuesta, que ofrece elementos para garantizar la integridad del sistema, creo que resulta importante que el proceso de digitalización a la hora de emitir el voto se produzca de manera gradual. No puede implantarse como una renovación total del modelo de votación introduciendo un sistema que resulta ajeno a la gran mayoría de la población. La integración del voto electrónico, incluso de voto *online*, debe realizase de manera escalada, dotando primero de una infraestructura suficiente a la administración electoral, aplicándose primero en consultas menores, preferiblemente no vinculantes, para que de esta forma la población comience a familiarizarse con el sistema de votación. Incluso, deberían convivir los sistemas de voto tradicional y electrónico, sea presencial o remoto, evitando de esta manera que algunos grupos de la población puedan verse desplazados del sistema de votación y, por ende, queden sin posibilidad de expresar su voluntad política.

Si bien es cierto que el principal inconveniente que se plantea en el voto electrónico a través de internet es la seguridad, no lo es menos que el elemento que inclina la balanza entre los sistemas tradicionales y las innovaciones presentadas, es la confianza depositada en el sistema. Mientras que el voto tradicional, con sus virtudes y defectos, se ha probado como un sistema en el que en un contexto normal los resultados son seguros, los sistemas de voto *online* no han podido, todavía, afirmar su seguridad en la práctica. Con el auge de la tecnología *Blockchain*, se abre una nueva posibilidad que, a mi juicio, otorga un grado de seguridad incluso superior al del sistema tradicional de votación.

Para finalizar, entiendo que, la tecnología *Blockchain*, se presenta como una buena alternativa a los sistemas de voto tradicional y voto electrónico presencial. Es una tecnología que permite desarrollar una red privada en la que se transmita la información de manera descentralizada y secreta, preservando de esta manera el anonimato del elector; asimismo, esta tecnología registra todos los cambios que se realicen por un votante, por lo que cualquier fallo puede ser rastreado; no puede introducirse ninguna información maliciosa dentro de la red, evitando así suplantaciones; se necesitan unas claves y códigos personales que garantizan que sea el sujeto con derecho a voto quien lo ejerza. Todo ello otorga un plus de seguridad, respecto de otras posibles alternativas dentro del marco del voto *online* que si se implementa con los medios necesarios y mediante un proceso de familiarización y preparación en la ciudadanía, con toda seguridad llevará a la obtención de la confianza precisa para su empleo,

ISSN: 2660-9231

elevando los estándares de seguridad, y con evidentes ventajas económicas y medioambientales a medio plazo.

Bibliografía

Alcántara Leiva, J. (2011). *La neutralidad de la Red y porqué es una pésima idea acabar con ella*. Disponible en: https://www.versvs.net/wp-content/libros/la-neutralidad-de-lared/jose-alcantara-la-neutralidad-de-la-red.pdf.

Arroyo Chacón, J. I. (2017). La innovación abierta como pilar del Gobierno Abierto. *Revista Enfoques. Ciencia Política y Administración Pública,* 15 (27), 13-41.

Barrio Andrés, M. (2022). *Manual de Derecho digital*. Valencia: Tirant Lo Blanch.

Cano Bueso, J. B. (2000). Democracia y tecnocracia: a propósito del voto electrónico. *Asamblea: Revista parlamentaria de la Asamblea de Madrid*, 3, 63-81. Disponible en: https://doi.org/10.59991/rvam/2000/n.3/763

Criado, J. I. (2021). La política de Administración digital en España. De los servicios públicos digitales a la gobernanza inteligente y administración pública 4.0. En C. Ramio, (coord.). *Repensando la Administración Pública. Administración digital y la innovación pública* (pp. 71-108). Madrid: INAP.

De Ávila Bula, M. (2019). *Proyecto de grado de Maestría Sistema de votaciones con Blockchain*. Disponible en https://repositorio.uniandes.edu.co/entities/publication/5e3b9e05-94a4-497b-82d8-64062fdb264e.

Pérez Medina, D. (2020). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. *Boletín Criminológico*, 26 (197), 1-24.

Fernández Riviera, R.M. (2001). El voto electrónico: El caso vasco. *Revista de Estudios Políticos (Nueva Época)*, 112, 199-236.

Fernández Rodríguez, J.J. (2007). El voto electrónico en la balanza. *Asamblea: Revista parlamentaria de la Asamblea de Madrid*, 17, 205-222.

Gálvez Muñoz, L. y Ruiz González, J.G. (2011). El voto electrónico y el test de calidad; o de cuatro bodas complicadas y un posible funeral. *Revista de Derecho Político*, 81, 253-274.

Gálvez Muñoz, L.A. (2009). Aproximación al voto electrónico presencial: estado de la cuestión y recomendaciones para su implantación. *Teoría y Realidad Constitucional*, 23, 257-270.

Gómez Oliva, A. y Pérez Belleboni, E. (2014). Metodología para la identificación de riesgos en sistemas de votación electrónica. *Elecciones*, 13 (14), 49-74.

González de la Garza, L. M. (2010). Voto electrónico por Internet y riesgos para la Democracia (II). *Revista de Derecho político*, 77, 213-249.

Hjálmarsson, F., Gunnlaugur K.H., Hamdaqa, M., y Hjálmtýsson, G. (2018). Blockchain- Based E-Voting System. En *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 983-986. Disponible en: https://ieeexplore.ieee.org/document/8457919

Lajpop Ajpacajá, K. A. (2022). Voto Electrónico con "Blockchain": La Unión entre la Tecnología y Sociedad. *Revista Científica del Sistema de Estudios de Postgrado de la Universidad de San Carlos de Guatemala*, 4 (1), 85-93. Disponible en: https://doi.org/10.36958/sep.v4i1.79.

Llamas Covarrubias, J. Z.; Llamas Covarrubias, B. A y Llamas Covarrubias, I. N. (2021). Características de validez en el voto electrónico mediante Blockchain. *Revista de Ciencia de la Legislación,* 10, s/p.

Martínez Dalmau, R. (2013). Constitución y voto electrónico. *Elecciones*, 12 (13), 137-160.

Mill, J. S. (1878), *El Gobierno representativo*. Disponible en: https://idus.us.es/items/e1d1fec6-877b-4860-8259-f63f97e984a8

Miró Llinares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Morales Rocha, V. M. (2009). *Seguridad en los procesos de voto electrónico remoto: registro, votación, consolidación de resultados y auditoria*, [tesis doctoral]. Universitat Politècnica de Catalunya. Disponible en: http://hdl.handle.net/10803/7043.

Pascual Ginard, M. d. P. (2021). *Voto por internet en democracia: estudio de los casos de Estonia y España*, [trabajo de fin de máster inédito]. Universitat Oberta de Catalunya. Disponible en: https://openaccess.uoc.edu/bitstream/10609/133349/6/pilarpascualTFM0621memoria.pdf

Pérez Alberdi, M. R. (2013). La delimitación del derecho de sufragio activo por el Tribunal Europeo de Derechos Humanos. *Revista de Derecho Político*, 88, 337-366.

Pérez Medina, D. (2020). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. *Boletín criminológico*, 26 (197), 1-24.

Presno Linera, M. A. (2011). *El derecho de voto: un derecho político fundamental*. Disponible en: https://presnolinera.files.wordpress.com/2011/10/el-derecho-de-voto-underecho-polc3adtico-fundamental-libro.pdf.

Presno Linera, M. A. (2016). Premisas para la introducción del voto electrónico en la legislación electoral española. *Revista de Estudios Políticos*, 173, 277-304.

Preukschat, A. (2017). Los fundamentos de la tecnología Blockchain. En Preukschat, A. (coord.). *Blockchain: la revolución industrial de internet* (pp. 23-30). España: Gestión 2000.

Rebato Peño, M. E. (1998). El Derecho de sufragio pasivo. *Parlamento y Constitución. Anuario*, 2, 227-265.

Tapscott A., y Tapscott D. (2017). *La revolución Blockchain*. Barcelona: Planeta.

ISSN: 2660-9231