INFORME SOBRE VOTO ELECTRÓNICO

Rafael Rubio Núñez. Catedrático Universidad Complutense.

Javier Hernando Masdeu. Profesor Universidad Villanueva

Documento elaborado en el marco del Convenio que la entidad pública empresarial Red.es ha suscrito con la agrupación de entidades formada por Political Watch (Fundación Salvador Soler), la Fundación Hay Derecho y la Fundación Haz, para impulsar la implementación de la Carta de Derechos Digitales en el ámbito de los derechos de participación [c-38/23-ot].

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

red.es

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Abstract

El informe analiza el potencial del voto electrónico (VE), el voto remoto por internet (VPI) y la tecnología *blockchain*. El VE promete aumentar la eficiencia y la participación, pero enfrenta desafíos críticos de seguridad y confianza. Tras un análisis de los estándares internacionales que exigen verificabilidad E2E, secreto y transparencia, se examinan casos de éxito y retrocesos y la posibilidad de recurrir a *blockchain* como solución. Se concluye que la implementación del VPI requiere previsión legal expresa y consenso, equilibrando accesibilidad con la garantía rigurosa del secreto y la verificabilidad.

1. INTRODUCCIÓN

1.1 Contexto. Tecnología y democracias

Una pregunta sobrevuela la vida política del siglo XXI: la digitalización ¿hará más confiable la democracia o cambiará su naturaleza y la de la misma política? (Rubio & Malikbayeva, 2023). Hace ya algunos años, a finales del siglo XX, y dentro de una ola de tecno optimismo que invadió el mundo, la tecnología se postuló como una forma de solución de muchos de los problemas de la democracia. Esta tendencia utopista alcanzó también a las elecciones y a los sistemas de votación. En ese contexto, el voto electrónico se presentó como la solución adecuada para algunos de los problemas que presentan los sistemas electorales, especialmente los referidos a la participación y a la agilidad en el recuento y publicación de resultados. Sin embargo, con el paso del tiempo, y la aparición de otras olas de tinte apocalíptico, que han pasado a señalar a la tecnología como la principal amenaza para la democracia, estos beneficios se han empezado a cuestionar, en contraste con desafíos como los de la seguridad y la confianza que son esenciales en cualquier proceso electoral y que pueden verse especialmente afectados cuando se implantan sistemas de votación electrónica.

Financiado por la Unión Europea NextGenerationEU

La transformación digital contemporánea que está ocurriendo en todo el mundo ha afectado a diferentes aspectos de la vida. Internet afecta claramente a "nuestra forma de pensar, de producir, de consumir, de negociar, de gestionar, de comunicar, de vivir, de hacer la guerra y de hacer el amor" (Castells, 1997 p. 25). Las transformaciones provocadas por la digitalización se consideran un componente básico de la cuarta revolución industrial. Además de su velocidad sin precedentes impulsada por los avances en la tecnología de la información, la comunicación mejorada, la ciencia de datos y los algoritmos, se cree que la transformación digital permite "eficiencia, eficacia, transparencia y apertura de la gobernanza, para promover la sostenibilidad y aumentar la rendición de cuentas y la participación civil" (Council of Europe, n.d.). El uso de la tecnología y la innovación fueron reconocidos como un imperativo para abordar los desafíos socioeconómicos globales, así como implementación de los Objetivos de Desarrollo Sostenible adoptados por la ONU en 2015 (Zambrano, 2017, p. 5).

En este contexto el debate entre apocalípticos e integrados se ha adueñado de la relación entre la tecnología y la democracia[1]. Desde una visión "tradicional", Internet no sería más que un canal de comunicación, más o menos extendido entre la población y cuya "virtualidad" reduce su impacto en la toma de decisiones. Esta visión, que es la que hoy en día sigue marcando las estrategias online de muchas instituciones políticas, ignora el impacto que este "canal" tiene en el resto de los canales y, sobre todo, las transformaciones que genera en las formas de comunicarse y organizarse de la sociedad.

Internet se ha convertido en el tejido de la sociedad. De ahí que plantearse su impacto exclusivamente en función de las posibilidades comunicativas resulta inadecuado. Es necesario ir más allá y plantearse, aunque sea brevemente, las transformaciones que las tecnologías están provocando, o no, en las organizaciones políticas y en las instituciones, considerando internet como un ámbito y no como una herramienta.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Se trata, pues, de plantear el debate sobre el impacto político de la digitalización y si la tecnología debería limitarse a hacer más confiable la democracia o está llamada a cambiar en un periodo relativamente breve la propia naturaleza de la política y de la misma democracia.

Como analizamos en profundidad (Rubio, Vela, 2017:19-31) los que consideran que sí, que la tecnología va a transformar el sentido mismo de la política, creen que a la disponibilidad de un volumen mayor de información y mayor transparencia, directamente relacionada, se uniría la participación, lo que se ha venido llamando la "recuperación del poder por parte de los ciudadanos" que, unirían al incremento de la información a su disposición la facilidad existente para relacionarse con otros ciudadanos, lo que aumenta su capacidad de recibir información y procesarla, su posibilidad de autoorganizarse y sus oportunidades para hacer llegar sus propuestas a las instituciones. Un cambio, en definitiva, de la forma de hacer política, que se ha traducido en el surgimiento de nuevas alternativas bajo estructuras políticas informales o poco habituales en el escenario electoral. Se estaría produciendo el paso de lo que Trippi (2004) denomina la política de la pasividad a la política de la actividad. De simples electores, los ciudadanos que lo deseen irían camino de convertirse hoy en parte de los procesos políticos. De ellos depende más que nunca que una propuesta logre movilizar a una masa social capaz de introducir sus intereses y objetivos en la agenda política e informativa. Este cambio de protagonistas hace que la política, reservada durante mucho tiempo a los políticos y a los medios de comunicación, conceda cada día más peso a los ciudadanos. La comunicación política, tradicionalmente asociada a la información y la propaganda, se va convirtiendo en la construcción de relaciones políticas permanentes. Una inmensa conversación de millones de personas hablando con millones de personas (*one-to-one*), con sus propias palabras y durante un largo periodo de tiempo; una conversación que cuando encuentra un objetivo claro (ya sea una elección o una toma de decisión por parte de las autoridades) se convierte en movilización social.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Esta concepción idílica de la democracia, que había puesto en la tecnología gran parte de sus esperanzas de regeneración, se va diluyendo con el paso del tiempo. Comienzan a cuestionarse elementos, fruto del impacto de la tecnología, como el exceso y la velocidad de la información que dificulta distinguir la verdad de la mentira, el excesivo peso de lo sentimental en la formación de la opinión pública, la transparencia absoluta que obstaculiza negociaciones y los acuerdos, la imposición de las mayorías frente a los derechos de las minorías, la falta de respeto a las instituciones jurídicas básicas para mantener el Estado de Derecho, la infoxicación (aun cuando la información es verídica y de calidad)…

1.2 Objetivos y justificación

En el contexto anterior el voto electrónico se presenta como un instrumento clave que puede condicionar la parte más visible de la participación, la relacionada con la toma de decisiones. En este sentido la posibilidad de votar desde cualquier sitio y en cualquier momento se ha planteado como una punto clave para la modificación del sistema democrático más allá de la celebración de elecciones.

2. MARCO TEÓRICO

2.1 Voto electrónico.

Desde un punto de vista técnico el voto electrónico formaría parte de las opciones de voto criptográfico o end-to-end verificable (EEV), un sistema que ofrece a cada votante una prueba que su voto ha sido contabilizado en el mismo sentido que fue emitido y que se complementa con el acceso a la información pública sobre la votación para que terceras partes puedan realizar comprobaciones. El Consejo de Europa estableció que su uso sólo sería recomendable si es seguro y confiable. En concreto, debería garantizar a los votantes la confirmación de su voto y la posibilidad de corregirlo si fuera necesario, respetando siempre el carácter secreto,

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

así como la seguridad y la transparencia del sistema (Council for Democratic Elections de la Comisión de Venecia, 2002). El equilibrio entre el secreto, la verificación y la libertad al emitir el voto son, de esta manera, los principales retos de estos sistemas de voto (Juels, Catalano y Jakobson (2005), aunque hay algunos (Torres García, 2022: 153-156) que consideran este equilibrio imposible, ya que siempre habrá que sacrificar uno de los principios básicos.

2.2 El voto electrónico remoto

El voto electrónico permite facilitar el voto, mejorar la velocidad del recuento, y a la vez puede permitir disminuir las posibilidades de fraude en el voto y el recuento. Sin embargo, una vez que se ha dado el primer paso de la digitalización se abren nuevas posibilidades que, al permitir ejercer el voto sin necesidad de acudir a la sede electoral, abre nuevas posibilidades especialmente al reducir los obstáculos físicos para el ejercicio del voto (de tiempo, de movilidad…), y permitir aumentar la participación. Con este objetivo el voto electrónico ha evolucionado incorporando tecnologías que permiten implementar sistemas de votación en remoto.

Este voto remoto, también conocido como voto en línea o voto por Internet (algunos autores se refieren a este procedimiento como "*i-voting*", para distinguirlo del voto electrónico presencial o "*e-voting*"), permite la emisión del sufragio desde cualquier lugar siempre y cuando se cuente con un dispositivo con conexión estable a Internet, como una computadora, o incluso, un teléfono inteligente. Se trata de una votación en la que ni el dispositivo utilizado ni el entorno físico en el que se encuentra están bajo el control de las autoridades electorales del país que recibe el voto, algo que no sucede habitualmente en los sistemas de voto electrónico.

2.3 *Blockchain*

La evolución del voto electrónico, y los obstáculos con los que se enfrentan sus distintas modalidades, parecen encontrar respuesta con la aplicación de la tecnología *blockchain*. Aunque no se trata de una modalidad de voto, propiamente dicha, en la evolución tecnológica del voto, tras la introducción de internet, la

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
Plan de Recuperación, Transformación y Resiliencia

aplicación de la tecnología *blockchain* merece un espacio propio. Su gran aportación es la confiabilidad en los registros y las transacciones, afectando al almacenamiento, la transmisión y la confirmación de datos, sin necesidad de realizar estas tareas a través de un sistema centralizado. Esto permite en el terreno electoral contar con un "registro" transparente y distribuido que puede permitir resolver algunas de las incógnitas que hasta ahora plantea el voto, en general, y el voto electrónico y el voto remoto, en particular. De ahí que se haya comenzado a utilizar esta tecnología en distintas fases del proceso electoral, desde la privacidad del censo hasta el recuento de votos.

En lo que se refiere al voto, en general, la contribución de *blockchain* se extiende al registro de votantes (censo) que puede ser objeto de filtraciones o de alteraciones, introduciendo o eliminando votantes en el mismo, lo que, si bien gracias al sistema de recursos no terminaría alterando el resultado final, sí que podría generar suficiente caos el día de la votación, provocando colas y disuadiendo a muchos para votar (algo que concentrado en lugares específicos sí que podría tener impacto electoral) y, en todo caso, aumentaría la desconfianza en el sistema. En segundo lugar, dentro de su aplicación al voto, *blockchain* podría mejorar la transmisión de votos de los colegios al registro central y la transparencia del recuento final, estableciendo un sistema de verificación de resultados y auditoría de los mismos. Por tanto, nos encontraríamos con una aplicación meramente instrumental que, si bien podría ayudar a mejorar la eficiencia del sistema y su seguridad, no supone cambios sustanciales en la forma de ejercer el voto, afectando sólo a su gestión interna.

Además de mejorar algunos aspectos del proceso de votación presencial, *blockchain* puede contribuir también a dar respuesta a algunas de las carencias del voto electrónico ya señaladas. Al estar basado en su capacidad para crear registros casi imposibles de modificar, que puede proteger el proceso de intromisiones externas, el uso de *blockchain* facilitaría un sistema de autenticidad del voto que garantizaría que ha sido emitido por su "propietario" y en el sentido pretendido por

este; el anonimato, desvinculando la emisión del voto con su contenido; la inalterabilidad del contenido; la posibilidad de los votantes de verificar que su voto ha sido contabilizado; y la auditabilidad tanto del proceso como de la plataforma de gestión por el que abrir el procedimiento a una auditoría general sin poner en riesgo el secreto imprescindible. Si a esto le añadimos la posible descentralización del sistema, eliminando intermediarios que puedan afectar a los resultados electorales, algunas de las ventajas señaladas se verían reforzadas. Así, se garantizaría aún más el anonimato, se evitarían las posibilidades de manipulación tanto de la autoridad central como de posibles hackers que pudieran introducirse en el sistema, y permitiría abrir la puerta a una mayor transparencia del sistema a distintos niveles (públicos, auditores, medios de comunicación), pudiendo ofrecer resultados prácticamente en tiempo real sin comprometer la seguridad del sistema. Además, los resultados de las votaciones serían almacenados en formatos abiertos y puestos a disposición de las instituciones para tomar decisiones. El carácter público y compartido de los datos en la cadena, especialmente en sistemas de código abierto, permitiría además, que cualquier persona pudiera verificar la integridad de la información, e incluso auditar la aplicación y contribuir a mejorar su seguridad.

Sin embargo, la utilización de la tecnología *blockchain* podría también, según algunos autores, introducir nuevas vulnerabilidades que no existían antes, sin ofrecer soluciones claras para los problemas de fondo que plantea el voto online. Estas nuevas vulnerabilidades, según sus críticos, supondrían un problema mayor que los que trataría de resolver (Blaze, 2017). Para estos la vulnerabilidad de los registros, a los que *blockchain* ofrece solución, no son la principal debilidad del voto electrónico sino la imposibilidad de garantizar la libre emisión del voto, algo que *blockchain* no puede garantizar. Además, una arquitectura *peer-to-peer* plantea dudas sobre la seguridad, distintas de las que hasta ahora se planteaban en el voto electrónico. Si un sistema controlado por la autoridad electoral ofrece vulnerabilidades vinculadas a esta autoridad central, un sistema construido sobre estructuras individuales o de organizaciones políticas, abriría otras vulnerabilidades. De esta forma, paradójicamente, algunos advierten esta inmutabilidad como una de

sus principales debilidades, al considerar que es imposible mantener la seguridad de esta información, y considerar que esto pondría en grave riesgo una información privada altamente sensible.

Para evitar estos peligros se plantean alternativas híbridas, que buscan solucionar esta debilidad a través de la centralización del proceso en una autoridad electoral. En este sistema alternativo los votos son enviados desde distintos dispositivos a una autoridad electoral, y contabilizados en un formato encriptado. El votante puede utilizar su clave para comprobar que su voto fue procesado adecuadamente, lo que reduciría el riesgo, pero no lo anularía como sostienen algunos que consideran este sistema, además, un riesgo para el secreto del mismo (Torres García, 2022).

En resumen, ante la crisis de credibilidad, la apuesta de *blockchain* es que cada vez sea menos necesario confiar y más sencillo verificar. Para lograrlo nos enfrentamos al dilema de reforzar el control del Estado para garantizar la integridad del proceso electoral o buscar nuevos caminos, utilizando la tecnología *blockchain*, para abrir y distribuir entre los ciudadanos el control de los sistemas de votación.

3. Metodología

Para realizar este estudio realizaremos una revisión bibliográfica y documental, con especial enfasis en su marco jurídico, a través de la exposición de los estandares internacionales existentes sobre el uso del voto electrónico. Distinguiremos en nuestro análisis entre el voto electrónico y el voto remoto, analizando por separado sus fortalezas y debilidades así como el estudio de casos siguiendo el método comparado, en el caso de que en algunos países, como Francia o México, existan experiencias de ambos tipos de tecnología hemos preferido presentarlas por separado. Finalmente, presentaremos una serie de conclusiones y recomendaciones sobre la implementación de estas técnicas de votación

4. La evolución del uso del voto electrónico

Desde mediados de los 90, cuando comienza la carrera por conseguir unas elecciones seguras a través de internet (Gibson et al., 2016), el voto electrónico se ha ido implantando en distintos países. Sin embargo, la evolución no está siendo rápida como se esperaba inicialmente y, por el contrario, se han producido retrocesos que han provocado que las autoridades sean realmente cautas a la hora de apostar por un sistema que podría reducir significativamente el coste de las elecciones y aumentar previsiblemente la participación (Gugliemi y Ihl, 2017).

Para conocer un poco mejor su evolución, nos remitimos a la base de datos de IDEA (Institute for Democracy and Electoral Assistance) sobre el estado global del voto electrónico (IDEA, 2023). Según la última actualización, de febrero de 2023, 34 de los 178 países analizados (un 19%) utilizan algún tipo de voto electrónico. En otros 27 (15%) se han realizado pruebas o están en desarrollo sistemas para implantarlo en el futuro. Conviene además anotar que en 11 países (un 6% del total) se han producido retrocesos, al abandonar el sistema de voto electrónico, una vez utilizado, como consecuencia de los errores detectados y los consiguientes problemas de confianza. El caso más señalado, como veremos con más detalle, es el de Alemania, pero también ha resultado fallida la introducción en Finlandia, Suecia, Irlanda o Japón. Una tendencia similar se observa también en el Compendio resumiendo prácticas de voto electrónico y otras aplicaciones de la tecnología procesos electorales en los países miembros de la UE (Compendium of e-voting and other ICT practices: non paper from the Commission services). En él se analizan con cierto detalle los casos de Bélgica, Portugal, Francia, Estonia, Irlanda, Lituania, Rumanía y la República Checa.

De estos 34 países señalados, 14 han ido implantando el voto por internet. Estonia y Emiratos Árabes Unidos son los dos casos más llamativos. En ambos se ofrece la posibilidad de votar en remoto a todos los ciudadanos convocados a las elecciones, mientras que en Australia, Corea del Sur, Canadá y Rusia se puede votar en remoto de manera limitada (en algunas regiones o en algunas elecciones locales). Otro conjunto de países ofrece la posibilidad de votar en remoto solo a los votantes que

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

se encuentren en el extranjero (de manera ordinaria o en circunstancias específicas como las misiones militares). Así lo hacen en Armenia, Ecuador, Estados Unidos, Francia, México, Nueva Zelanda, Oman, Pakistán y Panamá.

En el caso de *blockchain* podemos hablar de la puesta en marcha de distintas plataformas de votación y la puesta en práctica de alguna de ellas alrededor del mundo. Sus resultados nos permiten contemplar con esperanza las posibilidades de consolidar prácticas basadas o apoyadas en *blockchain* que podrían suponer un impulso a las modalidades de voto antes señaladas.

4.1 Estándares internacionales sobre el voto electrónico

El voto no es más que una parte del procedimiento electoral, sin embargo ocupa un papel central en el mismo al condicionar de manera determinante el recuento y, en consecuencia, el resultado. De ahí que para acercarnos a su estudio no podemos olvidar su marco jurídico. El marco más relevante es el que proporcionan el art. 21 de la Declaración Universal de Derechos Humanos de 1948 y el art. 25 del Pacto Internacional de Derechos Civiles y Políticos de 1966. Desde entonces, varias resoluciones o declaraciones de la Asamblea General de Naciones Unidas han enfatizado o subrayado algunos de los aspectos más importantes de estos preceptos, especialmente en materia de discriminación para ejercer el derecho al voto. También el Comité de Derechos Humanos de Naciones Unidas ha realizado glosas relevantes, como la conocida Observación General 25 (1996) sobre "El derecho a participar en los asuntos públicos, el derecho al voto y el derecho de acceso a cargos públicos en condiciones de igualdad".

Otros textos jurídicos de referencia en este campo son, por su detalle y por el momento de su aprobación, al final de la guerra fría, la Declaración de Copenhague de 1990 en el seno de la OSCE. Y, en Europa, el Código de Buenas Prácticas en materia electoral (CDL-AD(2002)023rev2-cor) aprobado por la Comisión de Venecia en 2002 que sigue siendo una referencia esencial.

Como es lógico, ninguno de estos documentos se refiere a la posibilidad de organizar sistemas de voto electrónico, pero los principios expuestos siguen siendo esenciales para orientar o validar la digitalización del voto.

Habrá que esperar hasta 2017 para que se publique el que a día de hoy sigue siendo el único documento intergubernamental relevante sobre voto electrónico, aprobado por el Comité de Ministros del Consejo de Europa en sesión del 14 de junio de 2017 (Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting). La Recomendación establece 49 estándares o requisitos para un sistema de votación electrónica agrupados en ocho apartados. La enumeración de los mismos es un buen resumen de los retos de cualquier sistema de este tipo:

- Sufragio universal
- Sufragio igual
- Sufragio libre
- Sufragio secreto
- Requisitos de organización y regulación
- Transparencia y observación
- Rendición de cuentas
- Fiabilidad y seguridad del sistema

Aunque la Recomendación del Consejo no sea vinculante, varios de los países que han organizado sistemas de voto electrónico la han utilizado como referencia.

También ha sido citada por algunas de las cortes constitucionales que han tenido que pronunciarse sobre la materia (Rodríguez Pérez, 2022)

El Consejo ha aprobado posteriormente otras *Guidelines on the use of information and communication technology (ICT) in electoral processes en 2023* (CM(2022)10-final) pero dejando claro que son unas directrices para aplicar en el uso de tecnología aplicada a cualquier fase del proceso electoral pero con la excepción expresa del voto y del recuento electrónico remoto, que no están incluidos, manteniendo en vigor lo establecido por la Recomendación de 2017.

4.2 Casos de uso

Tras esta visión general vamos a analizar con más detenimiento los casos de Bélgica, Brasil, Alemania, Países Bajos y Estonia, que, a la luz del sistema de votación y los problemas enfrentados, nos permiten una visión más integral de esta realidad.

4.2.1 Bélgica

En Bélgica se utiliza el voto electrónico presencial desde 1991. Tras las positivas pruebas iniciales de ese año, en 1994 un 20% de los electores optaron por el sistema electrónico. En 1998 la cifra se amplió a un 44% y se utilizó para las elecciones federales, regionales y europeas. En 2005 se tomó la decisión de mejorar el sistema incluyendo una garantía de registro en papel de voto y de depósito en urnas (*independent voter verifiable record IVVR or voter-verifiable paper audit trail VVPAT*)

Sin embargo, a pesar de la consolidación del sistema, en 2015, unas de las tres regiones que integran el país, Valonia, decidió abandonar el voto electrónico alegando razones de falta de transparencia y de excesivo coste. También resultaron decisivos los errores técnicos sucedidos en las elecciones de 2014.

Sorprende una decisión de estas características ya que el sistema ofrecía unas garantías básicas. El presidente de la mesa activa la máquina con una llave USB. Los miembros de la mesa comprueban la identidad del votante y le entregan una tarjeta

magnética que le permitirá operar en la máquina de votación, que se encuentra en una cabina que permite la privacidad de la operación. El elector utiliza la pantalla táctil para fijar sus preferencias y cuando ha terminado retira la tarjeta y la máquina imprime el voto con un texto que puede ser leído por el votante y con un código de barras que podrá leer el escáner de la cabina de votación. De este modo el elector puede comprobar que lo que la máquina ha impreso es lo que él había seleccionado en pantalla. A continuación, dobla el impreso dejando oculto el texto de lo que ha votado y entrega la tarjeta magnética en la mesa. Finalmente se dirige a la urna para votar. La urna tiene un obturador que solo se abre cuando el elector escanea su papeleta (boca abajo, para preservar la privacidad) Después del escaneo, el elector introduce la papeleta en la urna. Es importante notar que ningún dato sobre el votante es almacenado por el sistema. Por ese motivo la comprobación de la identidad se realiza en la mesa y la tarjeta que le entrega el presidente al votante solo sirve para activar la máquina. La papeleta que se imprime lleva un código que permite diferenciar cada voto pero que no tiene ninguna relación con la identidad del elector. La urna, después de escanear cada voto, inscribe los datos de este -encriptados- en una pareja de dispositivos USB. Estos serán enviados posteriormente a la sede de cada zona electoral para realizar el recuento.

Además, antes de cada proceso electoral el proveedor ha de realizar unos test previos para comprobar que las máquinas cumplen con los requisitos. A continuación la propia administración electoral realiza sus propios test con el asesoramiento de un proveedor tecnológico diferente al que proporciona el software y los sistemas de votación. Y en tercer lugar, el sistema es auditado por un tercero diferente e independiente de la administración pública (Colegio Federal de Expertos).

Este sistema presenta la ventaja de que el elector puede leer en su papeleta lo que ha votado. Y además, en caso de incongruencias en el recuento, la autoridad electoral puede acudir a la urna para realizar las comprobaciones oportunas. Y como hemos visto, queda garantizado el secreto del voto. Al buscar las causas de la decisión Valona encontramos críticas a la complejidad y el coste de la logística y a

los fallos técnicos que se producen con relativa frecuencia. Además, una parte relevante del electorado sigue desconfiando de la transparencia y fiabilidad del sistema a pesar de las garantías explicadas.

Por otra parte, el caso belga, por el largo tiempo transcurrido desde su implantación inicial y por su uso en elecciones de todo tipo, ha permitido realizar análisis más complejos desde el punto de vista de la ciencia política y no solo con la perspectiva más técnica del derecho electoral. El hecho de que, en un buen número de colegios electorales, se haya mantenido solo el voto en papel o se haya regresado a él después de unos años de voto electrónico permite hacer análisis y comparaciones interesantes.

Por una parte se ha tratado de estudiar en qué medida el voto electrónico favorece o no de hecho la participación. Y por otra parte, se ha considerado también si el voto electrónico influye en sí mismo de algún modo en las opciones políticas elegidas.

Con respecto a la participación, varios estudios citados por Dandoy (2021) y los suyos propios concluyen negativamente sobre la misma tanto en Valonia como en Flandes y en la generalidad del país en las elecciones desarrolladas entre 2006 y 2012, aunque las conclusiones son algo más matizadas por lo que se refiere a la región de Bruselas. En general, parece claro que la participación fue mayor en los cantones con votación tradicional con respecto a aquellos que habían pasado al sistema electrónico.

Por lo que se refiere a las candidaturas elegidas, la hipótesis que pretendía confirmarse es la de si los electores tendían a votar con más facilidad a candidaturas diferentes (cuando varias elecciones coincidían en la misma fecha) en los lugares en los que se utilizaba el voto electrónico. Los estudios de Dandoy (2021) y los citados por él no confirman esta tendencia.

4.2.2 Brasil

El caso de Brasil puede considerarse sorprendente. En un país en el que la confianza en las instituciones políticas se mantiene muy baja de modo constante resulta llamativa la amplia aceptación del voto electrónico desde su implantación a partir de 1996 (Avgerou, 2013). Desde entonces, con la relevante excepción de Jair Bolsonaro, especialmente en su candidatura presidencial de 2022, todos los partidos han respaldado el sistema y han aceptado los resultados incluso cuando han sido derrotados por márgenes estrechos.

El objetivo principal del sistema fue acabar con los larguísimos escrutinios. Por poner un ejemplo, en las presidenciales de 1989 se tardó casi una semana en terminar el recuento mientras que en la actualidad, cerca de dos horas después del cierre de los colegios electorales suelen estar computados cerca del 95% de los votos, lo que permite anunciar el resultado en la misma noche electoral.

También parece que el voto electrónico ha conseguido ampliar la base electoral, incluyendo a sectores que permanecían fuera del sistema por desconfianza o falta de acceso (Fujiwara & Fujiwara, 2015) (Schneider, 2021)

El elector accede a una máquina de votación que está desconectada de internet y se encuentra un teclado numérico y tres botones de colores para confirmar el voto, corregirlo o votar en blanco. Los candidatos desarrollan la campaña electoral presentando unos números. Estos representan a su candidatura o coalición, y son los que el elector deberá marcar en la máquina. Al final de la jornada, el presidente de la mesa retira los datos de cada máquina en un pendrive encriptado, que es conectado a otro dispositivo para enviar los datos al Tribunal Supremo Electoral, autoridad independiente encargada de la supervisión de todo el proceso y de realizar el escrutinio.

Hay que subrayar, sin embargo, algunos problemas (Abel, 2018) (Nicolau, 2019). El sistema brasileño no tiene un procedimiento de respaldo en papel como el descrito en el caso belga. El elector tiene que confiar en la seguridad del software de las

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

máquinas y del procedimiento de envío de los datos. En esencia, tiene que confiar en el Tribunal Supremo Electoral.

Como consecuencia de lo anterior en las elecciones de 2022 se consolidó una narrativa de fraude vinculada a la votación electrónica (muchas veces reutilizando material de anteriores elecciones) y que se concentraba en bulos como el del origen chino de las urnas, el uso exclusivo de las mismas en Brasil, Cuba y Venezuela, la entrega del código fuente a los venezolanos, o la imposibilidad de auditar las urnas. El ataque de hackers a las instalaciones del TSE y el TSJ alimentó la desinformación sobre la fragilidad del proceso de votación consiguiendo sembrar las sospechas sobre un sistema de votación, que contaba con una larga tradición en el país iberoamericano.

Estas narrativas se intensificaron según avanzaba la campaña electoral, reforzadas por los fallos técnicos e incidentes cibernéticos, la inestabilidad de la aplicación del E-tîtulo, o el retraso en la divulgación de resultados, pero gracias a la detección de estas narrativas, realizada meses antes, y a la construcción previa de contranarrativas, con distintas producciones audiovisuales, intervenciones públicas, publicidad presencial y actuaciones destinadas a desmontar estos bulos (como la auditoria ciudadana de las urnas electrónicas o el encargo a las fuerzas armadas de un estudio sobre la solidez del sistema), lograron reducir el impacto. Tras la elección se mantuvieron algunas narrativas que atacaban a ministros del TSE y defendîan el voto impreso como alternativa al mecanismo electrónico de voto. Estas sembraron el campo de cultivo de las movilizaciones que asaltaron la plaza de los tres poderes de Brasilia, en enero de 2023.

4.2.3 Alemania

Uno de los fracasos más sonados de los sistemas de votación electrónica es el que se produjo en Alemania en 2009. El Tribunal Constitucional declaró que cuando se utilizan máquinas de voto electrónico el principio constitucional de la naturaleza pública de las elecciones implica que "debe ser posible para el ciudadano

comprobar todos los pasos esenciales de la elección y de la certeza de los resultados sin un especial conocimiento técnico" y que esos requisitos no se cumplían con las máquinas empleadas en algunos estados en las elecciones al Bundestag de 2005 (BVerfG, Judgment of the Second Senate of 3 March 2009 - 2 BvC 3/07 -, paras. 1-166,) Conviene subrayar que el Tribunal no estableció que el voto electrónico fuera incompatible con los estándares constitucionales; tan solo que aquellas máquinas específicas no los cumplían. Aunque también es un hecho que no han vuelto a emplearse dispositivos electrónicos de votación en las elecciones alemanas.

Como hemos visto, un sistema como el utilizado por Bélgica tras las reformas de 2014 podría corregir lo señalado por el Tribunal Constitucional alemán por medio de un sistema *VVPAT o IVVR*.

4.2.4 Países Bajos

El caso holandés es otro ejemplo de entusiasmo inicial seguido de una decepción que lleva al abandono del voto electrónico.

En las elecciones provinciales de 1966 se utilizaron máquinas de voto electrónico por primera vez. La experiencia no fue positiva pero esto no desanimó al Consejo Electoral, que consideró que el problema había estado en unas máquinas norteamericanas que eran útiles con pocos candidatos pero presentaban problemas en un escenario tan fragmentado como el holandés. El sistema fue mejorado y también ampliado a más municipios, pero conservando siempre una doble votación electrónica y en papel. El objetivo era hacer más rápido y preciso el recuento pero sin perder la garantía y la trazabilidad del papel. Se perseguía además poder prolongar el horario de votación para facilitar la participación, lo que parecía posible si el escrutinio después del cierre del colegio electoral era más rápido.

El sistema tuvo críticas desde el principio pero fue en las elecciones de 2006 cuando se produjo la crisis final. Un grupo de particulares agrupado en una plataforma llamada “No confiamos en las máquinas de votación” realizó una fuerte campaña

pública que culminó en un programa de televisión en el que mostraron que podían manipular las máquinas de voto en varios sentidos suscitando dudas sobre el cómputo de resultados y sobre el secreto del voto. El gobierno, además, no fue capaz de dar una respuesta clara al asunto y optó por organizar dos comisiones de estudio para intentar encontrar una solución. Finalmente, en 2008 se optó por abandonar el sistema y volver al sistema de voto en papel, que es el que sigue utilizándose (Loeber, 2008) (Jacobs & Pieters, 2009) (Spoormans, 2019) (Duenas-Cid, 2024)

4.2.5 Francia

El marco legal que rige el voto con máquinas en Francia (denominadas "máquinas de votar") fue establecido inicialmente por un decreto (n° 64-1086) del 27 de octubre de 1964. Pero la reforma legislativa llegaría con la incorporación al Código Electoral mediante una ley del 10 de mayo de 1969 que incorporaba el nuevo artículo L. 57-1.

El uso de ordenadores de voto quedaba restringido legalmente a municipios de más de 3.500 habitantes. La autorización de los modelos específicos recae en el Ministerio del Interior. Ejemplos de modelos autorizados fueron la versión de NEDAP, el modelo "iVotronic" de ES&S, y el modelo "Point & Vote" de Indra Sistemas SA.

En 2003 se aprobó un reglamento que fijaba las condiciones de homologación. Este reglamento ha sido objeto de críticas por ser superficial y por permitir que el programa de software utilizado en las máquinas fuera secreto, amparado por el secreto industrial y comercial. Esta protección legal del código fuente impide a los ciudadanos examinar el sistema, socavando el principio de transparencia (Enguehard 2007)

La principal objeción al voto electrónico presencial radica en que el control del voto escapa a los ciudadanos. A diferencia del proceso tradicional con papeletas de papel, donde el votante deposita una papeleta en una urna visible, el procedimiento

electrónico no ofrece al elector la posibilidad de verificar en ningún momento que su elección ha sido registrada correctamente. El proceso estándar implica que el ciudadano selecciona en la pantalla, confirma su elección y luego firma la lista electoral. El recuento electrónico se realiza de manera automática y opaca, sin permitir la participación de los ciudadanos escrutadores. Una crítica que se repite es que los ordenadores de voto franceses no están obligados a imprimir un boletín de papel verificado por el elector. Esta ausencia de una traza física hace que el sistema sea totalmente inverificable. Sin una prueba física que pueda ser recontada manualmente, resulta imposible detectar los fallos de funcionamiento (Daoudi 2021)

Adicionalmente, estudios comparativos en elecciones presidenciales y legislativas entre 2007 y 2017 han revelado que las estaciones de voto electrónico presentan una tasa de error en las diferencias entre votos emitidos y firmas registradas considerablemente más alta (hasta 4,4 veces superior en la segunda vuelta presidencial de 2007) que las estaciones que utilizan papeletas de papel (Enguehard 2020)

La introducción de las máquinas de votación ha forzado a las altas jurisdicciones francesas (Consejo Constitucional y Consejo de Estado) a adaptar la legislación electoral tradicional a las nuevas tecnologías.

En general, la jurisprudencia electoral (en sus últimas instancias, del Consejo de Estado o del Consejo Constitucional) ha exigido a los recurrentes que prueben que la irregularidad o el mal funcionamiento denunciado (sea un error aritmético o un defecto técnico) pudo alterar el escrutinio y modificar el resultado. Este requisito se ha convertido en una barrera casi insuperable para los oponentes al voto electrónico. Sin la posibilidad de realizar un recuento manual o de acceder al código fuente, resulta imposible demostrar ante el juez que un fallo técnico afectó el resultado (Guglielmi 2017). El juez se remite a menudo al hecho de que el modelo está "homologado por el Ministerio del Interior", declarando así su legalidad (Daoudi 2021) En general, las resoluciones renuncian a entrar en las cuestiones técnicas y confían en las homologaciones.

Lo que sí parece claro es que esta modalidad de voto ha generado nuevos motivos de impugnación que se focalizan en aspectos técnicos y ergonómicos. Ejemplos incluyen la dificultad de lectura en pantalla debido al alto número de listas o la afectación a la igualdad del voto debido a la reducción gráfica de los nombres de los candidatos en las interfaces. La automatización tiene potencial para transformar los intentos de fraude electoral, ya que se han constatado lo que a menudo se llaman "ataques" informáticos. Algunos técnicos creen haber demostrado vulnerabilidades como el Denial of Service (DoS), que bloquea la máquina, o el vote-stealing (robo de votos), que modifica la distribución de sufragios entre candidatos sin alterar el total de votos expresados, volviendo la manipulación indetectable (Daoudi 2021) (Enguehard 2020)

En cualquier caso, y aunque las impugnaciones judiciales hayan tenido un éxito escaso, han sido suficientes como para causar el bloqueo del sistema. El experimento francés con el voto electrónico presencial se encuentra en una situación de suspensión desde la moratoria de 2008, que impide a nuevos municipios adoptar esta tecnología (Daoudi 2021)

4.2.6 México

Sobre el caso de México, resulta de gran interés el “Informe final de actividades sobre el PIT-VMRE” (Plan Integral de Trabajo del Voto de las Mexicanas y los Mexicanos Residentes en el Extranjero para los Procesos Electorales Federal y Locales 2023-2024) aprobado por el Consejo General del INE el 29 de agosto de 2024 (disponible en https://repositoriodocumental.ine.mx/xmlui/handle/123456789/176656) En él se contiene información relevante sobre el uso reciente del voto electrónico.

El voto electrónico (e-voto) se despliega en México principalmente en dos modalidades: el Voto Electrónico Presencial (VEP), mediante el uso de la Urna Electrónica del INE en casillas específicas, y el Voto Electrónico No Presencial

(VENP) o Voto por Internet (VPI), enfocado primariamente en los ciudadanos mexicanos residentes en el extranjero (VMRE).

El modelo VEP se basa en la Urna Electrónica desarrollada por el INE, utilizada en pruebas piloto vinculantes desde 2020 en Procesos Electorales Locales y Concurrentes.

Para el Proceso Electoral Concurrente (PEC) 2023-2024, el INE determinó el uso de la Urna Electrónica modelo 7.0. Este despliegue se concentró en 71 casillas especiales, distribuidas en la Ciudad de México (44 casillas) y en Nuevo León (27 casillas, en municipios como Monterrey, Apodaca, San Pedro Garza García, San Nicolás de los Garza y General Escobedo).

La Urna Electrónica modelo 7.0 posee un diseño modular que incluye el módulo de votación (pantalla), el módulo de impresión y el módulo de respaldo de energía. Es un dispositivo de pantalla táctil que opera de manera completamente independiente y no tiene conexión a internet. Esta característica es fundamental para garantizar que los votos permanezcan en su sistema interno y no puedan ser alterados de forma remota.

El sistema incorpora garantías de verificación y agilidad:

1. Testigo del Voto: Permite al elector corroborar su selección en la pantalla antes de emitir su sufragio, y después, revisar que se haya registrado correctamente mediante un "testigo del voto" impreso en papel. Estos testigos impresos son depositados en un contenedor interno.
2. Agilidad en el Escrutinio: El sistema obtiene los resultados de la votación de forma automática, lo que evita errores aritméticos y reduce el tiempo empleado en el escrutinio y cómputo, además de simplificar el llenado de formatos y el cierre de la casilla.

La operación requiere el uso de tarjetas de activación: la tarjeta blanca (PMDC) para el Presidente de la Mesa Directiva de Casilla y tarjetas rosas para la votación, que se

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

inhabilitan temporalmente después de cada uso. El INE enfatiza que la Urna Electrónica cumple con las medidas de seguridad y transparencia establecidas.

La implementación del VEP requiere que el personal de apoyo esté presente de manera fija en los lugares con urna electrónica. Las contingencias incluyen fallas de energía eléctrica (para lo cual se traslada una planta de luz manual), pérdida o alteración de sellos, fallas totales de la urna (requiriendo reemplazo), y problemas con el papel térmico.

En cuanto a la fiscalización, la Auditoría Superior de la Federación (ASF) revisó la gestión de las TIC del INE en 2021. Aunque se concluyó que el INE cumplió en términos generales con las disposiciones legales, la evaluación del Gobierno y Gestión de las TIC determinó que el 49.6% de los procesos tenían un bajo nivel de cumplimiento o era parcial. Esto se identificó como un riesgo mayor en la entrega operativa y el soporte de los servicios de tecnología y seguridad de la información.

En resumen, en México el VEP (Urna Electrónica) ofrece ventajas claras en la eficiencia y la verificación local (testigo impreso), mitigando riesgos de ciberataques gracias a su funcionamiento offline. No obstante, la fiabilidad institucional se ve comprometida por las deficiencias en la gobernanza de TIC señaladas por la ASF (casi el 50% de los procesos de TIC con bajo o parcial cumplimiento en 2021).

4.2.7 República Dominicana.

En el mes de febrero de 2020 la JCE de República Dominicana decidió suspender las elecciones por problemas relacionados con el voto electrónico que afectaron a 18 distritos electorales, (el 62 por ciento de los votantes), el gravíísimo incidente dio lugar a un esclarecedor informe de la Organizacióón de Estados Americanos que nos aporta algunas pistas. "La falla determinante (...) consistía en que en un número considerable de las máquinas de voto automatizado no se habían cargado las boletas (papeletas) de manera correcta", de modo que "un gran número de las urnas

distribuidas en el país no contaban con la oferta electoral (candidaturas) correctamente instalada", explicó la OEA. De ahíí que se atribuya la responsabilidad a “la mala gestión del área informática de la JCE durante las elecciones".

El problema principal fue "el mal diseño del software" que "no tenía mecanismos de control de integridad de la oferta electoral y, por lo tanto, era incapaz de detectar cualquier tipo de problema que se pudiera haber presentado en el proceso de descarga de las boletas electrónicas", esto se vió agravado por "la inexistencia de procedimientos formales de prueba del software", lo cual "impidió que se detectase el defecto durante la fase de pruebas". Además, denunció que la JCE "decidió utilizar mecanismos de transferencia de la información que no solo no estaban previstos sino que tampoco fueron evaluados" para cargar las candidaturas en las máquinas de votación al darse cuenta de que con el sistema que había ideado "no llegarían a finalizarlo antes de la fecha prevista" para los comicios.

La improvisación llevó a los técnicos a usar una red distinta de la prevista con el fin de paliar la falta de tiempo, con el infortunio de que la nueva red era menos potente de lo necesario y "se interrumpió la descarga quedando la oferta electoral incompleta".

De ahí que se señale "la ausencia de protocolos y la falta de aplicación de buenas prácticas" durante las elecciones, pero "el equipo auditor no encontró evidencia de ataques externos, sabotaje o intento de fraude".

4.2.8 España

El marco normativo

La legislación electoral española (LO 5/1985, en adelante LOREG) no prevé un sistema electrónico de votación para ninguno de los procesos electorales que regula. Desde el principio, el procedimiento de votación ha pivotado sobre dos instrumentos: papeletas y urnas. Actualmente, la LOREG configura la expresión del

sufragio a través de papeletas de votación introducidas en un sobre y depositadas en una urna (artículo 86.2 LOREG). Este modelo material de votación solo puede ser modificado por la mayoría absoluta del Congreso de los Diputados.

En consecuencia, el uso de cualquier modalidad de voto electrónico, ya sea presencial en urna electrónica o por internet, no es legal en España para los procesos electorales generales o referéndums. La Ley Orgánica 2/1980, sobre regulación de las distintas modalidades de referéndum, también establece que la votación debe realizarse mediante papeletas y sobres ajustados a un modelo oficial.

Conviene, no obstante, notar que la LOREG no impone un voto presencial. Lo que se imponen son las papeletas y las urnas. Por ese motivo no hubo inconveniente para introducir un voto por correo. Y también de ahí puede deducirse que no hay principios relevantes del derecho electoral español que resulten por definición incompatibles con el voto electrónico. Los únicos límites claros son los establecidos en los preceptos constitucionales referidos al voto. El sufragio ha de ser "universal, libre, igual, directo y secreto" (art. 68.1 de la Constitución) y los ciudadanos tiene "derecho a acceder en condiciones de igualdad a las funciones y cargos públicos" (art. 23.2 de la Constitución)

En cualquier caso, la LOREG no excluye por completo la posibilidad de acudir a sistemas de voto electrónico remotos o presenciales. Por un lado, las Comunidades Autónomas tienen la competencia para regular los procesos electorales que integran sus parlamentos. Por otra parte, las administraciones pueden también realizar experimentos sin validez jurídica que sirvan para probar los sistemas y para explorar posibles vías de actuación. Como veremos, las dos posibilidades han sido utilizadas.

El informe del Consejo de Estado de 2009

El 24 de febrero de 2009 el Consejo de Estado español emitió un largo informe sobre la reforma de la LOREG . En dicho informe se hacía referencia al voto electrónico con un breve análisis de derecho comparado y un repaso de las experiencias que habían tenido lugar en España a ese respecto. En 2004 el Ministerio del Interior realizó una prueba con 300 electores de 3 mesas electorales, a los que se daba la posibilidad de votar en ordenadores situados junto a las mesas tras ejercer su derecho al voto en las urnas convencionales. También sin validez legal, en 2005 se realizó una prueba más amplia en el referendum para la ratificación de la Constitución Europea. En esa ocasión se ofreció la opción en un municipio grande de cada una de las 52 provincias españolas, lo que daba la opción de votar electrónicamente a unos 2 millones de electores. El resultado fue poco alentador: solo un 0,54% de los votantes utilizaron las urnas digitales. El informe del Consejo hace notar que la información a los electores fue escasa y también diversos fallos de seguridad y de vulneración de secreto de voto. También se realizaron pruebas -sin valor legal- en algunos municipios en las elecciones autonómicas de Cataluña en 1995 y en 2003. Lo más interesante de la última prueba es que se incorporó también un voto remoto para los catalanes residentes en un grupo de países. El índice de participación fue muy bajo. También se realizaron pruebas similares en Valencia, Baleares y Andalucía.

Como se ha dicho, las Comunidades Autónomas tienen capacidad para regular sus procedimientos electorales. El informe se refiere también a la ley 15/1998, de 19 de junio, que reformó la Ley 5/1990 de Elecciones al Parlamento Vasco. La reforma incorporó un Capítulo X específico (arts. 132 bis a 132 septies) para regular el procedimiento de votación electrónica. Sin embargo, la Disposición Final 1.ª difería la entrada en vigor de este procedimiento hasta que se produjera una decisión posterior del Parlamento Vasco. Y dado que dicha decisión no se ha tomado, el caso vasco es solo un ejemplo de regulación.

El informe concluye haciendo una valoración conjunta de todas estas pruebas. En primer lugar se ponderan las potenciales ventajas del voto electrónico, sobre todo en

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

relación a la ampliación de la participación y a la celeridad en el recuento. Pero también se hace referencia a los problemas de control y de seguridad que se han planteado. Y quizá lo más interesante sea la referencia final a la necesidad del cambio. El Consejo considera la cuestión de si los beneficios son proporcionales a los costes y a los riesgos. Y parece concluir que en el caso de España, cuyo sistema electoral funciona razonablemente bien, la respuesta no es clara.

El informe de la Junta Electoral Central de 2016

El órgano que encabeza la administración electoral en España es la Junta Electoral Central, compuesta por Magistrados del Tribunal Supremo y Catedráticos designados por los partidos políticos con representación parlamentaria. El 16 de noviembre de 2016 dicha Junta emitió un informe sobre la regulación del voto de los electores españoles que residen o se hallan en el extranjero. Y en él se hace una referencia amplia a la posibilidad, que se estaba discutiendo, de incorporar el voto por internet para ese grupo específico de votantes.

Lo primero que hace la Junta es afirmar que no hay impedimento constitucional para establecer tal tipo de votación. La Constitución no se refiere a la cuestión pero tampoco la prohíbe. Y del mismo modo que se introdujo el voto por correo podría introducirse el voto por internet, siempre que se respetaran las garantías que la Constitución sí hace explícitas para el ejercicio del sufragio.

A continuación, la Junta se plantea la idoneidad y la necesidad de la incorporación de un voto remoto por internet para los electores ausentes. Y en este caso, y a la vista de las escasas cifras de participación en esa parte del cuerpo electoral, considera que la medida podría ser idónea y necesaria.

Por lo que se refiere a las garantías constitucionales, la Junta las examina una por una (sufragio universal, libre, igual, directo y secreto) y considera que no parece

imposible salvaguardarlas, aunque se planteen reservas importantes a las que habría que atender debidamente al diseñar el sistema, siguiendo las recomendaciones o estándares fijados a este respecto por organismos internacionales como el Consejo de Europa. Y en cualquier caso, la Junta nota también que el sistema de voto por correo no está tampoco exento de problemas.

La Junta concluye que la implantación del voto remoto sería idónea y también necesaria, pero también excepcional y dirigida únicamente a los electores ausentes, y en cualquier caso alternativa a otras vías convencionales, que, mejoradas, deberían mantenerse a disposición del elector. Se insiste también en que "en todo caso, la implantación del sistema requeriría un amplio debate público, destinado a asegurar un grado muy elevado de consenso político y a afianzar la confianza en el sistema electoral en su conjunto".

5. ¿EL VOTO REMOTO COMO SOLUCIÓN?

5.1 Estándares internacionales para el voto remoto

Los estándares internacionales para el voto por internet han sido trazados principalmente por organismos como el Consejo de Europa y la OSCE (Organización para la Seguridad y la Cooperación en Europa). Estos organismos no imponen el voto por internet, pero sí han definido un modelo ideal con características que aseguran su idoneidad para manifestar la voluntad democrática de los electores.

Los documentos clave que establecen este marco internacional incluyen:

El Código de buenas prácticas en materia electoral (2002).
El Informe acerca de la compatibilidad de voto a distancia y voto electrónico con los estándares del Consejo de Europa (12-13 de marzo de 2004), elaborado por la Comisión de Venecia.

La Resolución del Comité de Ministros del Consejo de Europa (30 de septiembre de 2004), que se materializó a partir del informe de la Comisión de Venecia.

La publicación E-voting Handbook (2010).

Las Guidelines on transparency of e-enabled elections (2011).

El Handbook For the Observation of New Voting Technologies (2013), publicado por la OSCE.

5.1.1 Ventajas y riesgos

Las ventajas del voto por internet son fundamentalmente facilitar la emisióón del voto desde cualquier lugar, permitiendo ampliar la participación, especialmente en aquellos que se encuentran fuera de su país, con las dificultades que esto supone de cara a la emisión del voto. Por ejemplo en España en las elecciones generales de 2016, solo el 6,30% de los inscritos en el CERA vio sus votos escrutados, cantidad que se mantuvo muy similar en 2019 y que, tras la reforma del sistema, alcanzó el 10% de los votantes, una cantidad que sigue siendo muy escasa. Esta situación de hecho vulnera la igualdad de los nacionales que viven fuera de sus fronteras, afectando a la igualdad.

En lo que se refiere al riesgo, los expertos advierten que no existe hoy en día ninguna tecnología que pueda garantizar la certeza absoluta de un sistema de voto por Internet. El VPI se enfrenta a riesgos inherentes a la tecnología que condicionan la libertad y el secreto del voto. Estos riesgos se dividen en:

1. Riesgos para el Usuario: La votación se realiza fuera del entorno seguro de la casilla, exponiendo al ciudadano a la coerción por parte de terceros (familiares, empleadores). Además, los dispositivos del votante son vulnerables al hackeo mediante *malware*, lo que permitiría cambiar el voto antes de su cifrado y envío, sin que el usuario lo note.
2. Riesgos del Sistema: El sistema es vulnerable a ataques externos (DDoS, robo de información) y a fraudes internos. Una sola persona con acceso puede manipular la elección y borrar sus huellas, haciendo el fraude "invisible".

Esta situación se conoce como el "dilema secreto-integridad". Para proteger el secreto, la identidad del votante se separa del voto cifrado (el sistema opera como una caja negra). Sin embargo, para verificar la integridad (saber si el voto se contó correctamente), se requerirían recibos detallados del sentido del voto, lo que vulneraría el secreto. La única opción que queda al votante es confiar en que el sistema hace lo que las autoridades dicen.

Las auditorías suelen ser centralizadas y sectorizadas por las autoridades electorales, lo que impide que el código sea de código abierto (*open source*) y que se realicen pruebas de penetración y recompensa por expertos independientes. Además, los hallazgos de seguridad no se suelen hacer públicos, sino que se comunican de forma privada a las unidades técnicas del INE, operando bajo una lógica de *"security by obscurity"* (seguridad por oscuridad).

1. Refuerzo Legal y Consenso Político: Se debe enfatizar que la introducción del VPI debe realizarse mediante una previsión legal expresa que asegure el apoyo político de la medida. No se considera sensato forzar la literalidad del artículo 75.12 de la LOREG (Ley Orgánica del Régimen Electoral General) para introducir modificaciones sustanciales por vía reglamentaria. Es fundamental un amplio debate público para asegurar un grado muy elevado de consenso político y para afianzar la confianza en el sistema electoral en su conjunto.
2. Mitigación de la Brecha Digital y la Universalidad: Aunque el VPI mejoraría la participación, se debe reconocer que la brecha digital podría introducir una desigualdad material extraordinaria entre los residentes ausentes "duchos" en la red y aquellos que no lo son. Para mitigar esto, se recomienda mejorar los procedimientos alternativos (voto postal o consular).

5.1.2 Principios y Garantías

La Recomendación del Comité de Ministros del Consejo de Europa, en su Apéndice I, establece los principios esenciales y las garantías procedimentales que deben regir el sufragio electrónico:

a) Principios (Características del Voto):

El Derecho internacional de los derechos humanos también fija un mínimo de protección obligatoria para los Estados suscriptores. El Artículo 25 del Pacto de Derechos Civiles y Políticos (1966) y la Declaración de Derechos Humanos de la ONU (1948) establecen que la voluntad del pueblo debe expresarse mediante elecciones auténticas que se celebren periódicamente por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad de voto. Por otro lado, la Recomendación del Consejo de Europa menciona Universalidad, Igualdad, Libertad y Secreto. El Derecho constitucional español, además, incluye el principio de Directo.

Universalidad. La universalidad implica el potencial ejercicio del sufragio por todos los electores. Un problema con el voto por internet es que, aunque facilita la participación de electores con dificultades (como los residentes ausentes), requiere conocimientos mínimos de las nuevas tecnologías y acceso a internet. Además, la universalidad se relaciona con el control potencial de cualquier elector sobre el procedimiento completo, incluyendo la identificación, el depósito y el recuento (lo que se denomina publicidad). En el voto por internet, este control desaparece, ya que el proceso pasa a ser monopolizado por expertos informáticos, lo que conlleva una cierta privatización del proceso electoral. Si se infringe esta capacidad de control ciudadano, el sufragio por internet podría ser inconstitucional por falta de transparencia, como sugirió el Tribunal Constitucional Federal alemán.

Igualdad. El voto telemático debe ser equivalente al voto presencial para asegurar la igualdad del sufragio. Si se utiliza como alternativa para los residentes ausentes (CERA/ERTA), su introducción podría aliviar la carga y disipar la desigualdad material que enfrentan con el sistema actual, haciéndolos más parecidos a los residentes nacionales. No obstante, se plantea una duda en relación con la brecha digital. Solo los electores con acceso a internet y capaces de manejarlo se beneficiarían de esta alternativa. Esta situación podría introducir una desigualdad

material extraordinaria entre los residentes ausentes "duchos" en la red y aquellos que no lo son.

Libertad. La libertad del votante se asegura clásicamente en un entorno vigilado y seguro (el colegio electoral), donde se comprueba su identidad y se garantiza que no está siendo coaccionado. En el voto por internet, el elector no vota en un entorno asegurado por el poder público. La identificación es electrónica, lo que no da plena garantía de que otro no use las claves del votante o de que el votante no esté bajo presión externa. En estos casos, la responsabilidad recae por entero en el elector.

Secreto. El secreto del voto es crucial y está intrínsecamente ligado a la libertad. La debilidad del voto por internet es justamente la ausencia de una garantía absoluta de la reserva del voto. Cuando se habla del voto electrónico remoto, es frecuente plantear la paradoja de la amplia aceptación del uso de banca electrónica en remoto en contraste con la desconfianza que genera el uso electoral de técnicas parecidas. Pero suele obviarse una diferencia esencial entre ambos procedimientos: el secreto del voto. En la información bancaria no hay ningún inconveniente en que el banco sepa qué hacemos con nuestro dinero. Más bien al contrario, se trata de asegurar que el banco sepa exactamente qué es lo queremos hacer con nuestro dinero. Pero en el caso de la votación en remoto hay que jugar con un factor que complica enormemente las cosas: el gestor del sistema tiene que permanecer ciego ante lo que ha votado el elector. Y eso no solo durante el acto de la votación sino también en el recuento posterior y en las impugnaciones o chequeos que hayan de realizarse.

El procedimiento clásico para asegurar el secreto del voto son las cabinas electorales. Como es sabido, para que esto funcione bien es necesario que se cumplan una serie de requisitos anteriores y posteriores. En el momento de la votación, es necesario asegurar que el local electoral tiene unas cabinas lo suficientemente amplias como para contener las papeletas de todas las candidaturas y los sobres en los que estas han de ser introducidas. Además, el

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

diseño de la cabina debe permitir que el elector quede libre de las miradas del resto de personas que se encuentren en el local. Es un procedimiento simple y una garantía fácil de comprender para los ciudadanos. Pero no está exento de problemas. Es necesario que esas condiciones se mantengan a lo largo de toda la jornada de votación. Y lo habitual es que en cualquier elección importante, con miles de locales, sucede que las papeletas se agotan o son sustraídas en algún momento de la jornada. O que la cabina se deteriora y no se cumplen los requisitos de privacidad. Pero obviamente, el secreto del voto en papel no se ve afectado solo por los inconvenientes de las cabinas electorales. La compra de votos es relativamente sencilla. Basta con entrar en el local con una papeleta que ha sido introducida en el sobre previamente -fuera del local- en presencia de la persona que ha pagado por el voto. Después, solo es necesario que alguien observe en el interior que el votante no altera la papeleta antes de depositarla en la urna. Para tratar de evitar esto, se puede obligar a todo el mundo a entrar en la cabina y permanecer en ella un tiempo mínimo para asegurar la privacidad. En la práctica, esto dificulta la fluidez del proceso y tampoco asegura que la compra no vaya a producirse. Es sencillo utilizar un dispositivo móvil para fotografiar o retransmitir en vídeo desde la cabina y demostrar así que se ha votado lo que estaba pactado.

Sobre la garantía del secreto en el voto electrónico no parece haber un consenso claro. De hecho, es amplio el número de autores que consideran incompatible el secreto de sufragio y los sistemas de votación electrónica (Rodríguez Pérez, 2022).

Cualquier sistema de votación en la red debe preservar el secreto y el anonimato del voto, logrando la desconexión entre el elector identificado y el sentido del voto. Los sistemas por internet deben encriptar el voto y separarlo del elector que accedió con una clave personal, replicando el proceso de la urna convencional donde una persona identificada deposita un voto que se vuelve anónimo.

Directo (Exigencia Española). En el caso de España la propia Constitución establece que el voto debe ser directo. Esta característica se considera salvaguardada en el voto por internet porque el sufragio encriptado se desencripta para el recuento y se contabiliza a los mismos efectos que el voto presencial.

b) Garantías Procedimentales:

El Consejo de Europa también exige garantías procedimentales que el sufragio electrónico debe respetar: Transparencia, Verificación, Seguridad y Fiabilidad.

Transparencia. La transparencia es esencial. En el voto por internet, hay una notable ausencia de publicidad en comparación con el voto convencional. Dado que el proceso se desarrolla por medios electrónicos, el ciudadano común no puede verificar la regularidad del funcionamiento del sistema, dificultando la transparencia.

La falta de transparencia es una desventaja importante que solo se vería superada si el voto por internet fuera el remedio excepcional para hacer posible el pleno ejercicio del derecho fundamental de sufragio activo, como ocurre con los residentes ausentes.

Seguridad y Fiabilidad. El consenso internacional exige que el sistema cumpla con cualificaciones jurídicas y técnicas específicas. La seguridad es un factor clave, ya que los sistemas de voto en la red pueden ser vulnerables a ataques externos (hackers) o manipulación interna. Se requiere un sistema completo de garantías y previsiones técnicas para contrarrestar estas amenazas, tales como:

Control sobre los programas que posibilitan la votación.
Ubicación y control sobre el servidor.
Seguridad de internet en los países donde se emite el voto.
Medios técnicos para garantizar la personalidad del votante y que el sufragio se emita sin coacciones.
Planes de emergencia en caso de fallos del sistema.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Si no se presupone la seguridad del sistema técnico de la red, no cabe imaginar su viabilidad constitucional.

Verificación. La verificación es necesaria para asegurar la integridad del proceso y detectar cualquier manipulación. El procedimiento telemático debe permitir su verificación de forma independiente. A menudo, esta tarea de control y fiscalización técnica queda en manos de expertos informáticos o empresas privadas de auditoría (lo que acentúa la sensación de "privatización" del proceso). Por ello, se recomienda una fiscalización técnica rigurosa por agentes diferentes a quienes prestan el servicio. Un requisito fundamental es que el elector pueda comprobar que su voto ha sido contado y que lo ha sido con el sentido que él le dio.

5.1.3 Requerimientos Técnicos

Existe un consenso internacional acerca de las cualificaciones jurídicas y técnicas que la modalidad de voto por internet debe cumplir. La resolución del Comité de Ministros del Consejo de Europa de 2004 destaca en su Apéndice III los requerimientos técnicos del sistema para que cumpla con los estándares legales del Derecho internacional de los derechos humanos.

En general, la implementación del voto por internet exige un sistema completo de garantías, incluyendo:

Control sobre los programas que posibilitan la votación.
Ubicación y control sobre el servidor.
Seguridad de internet en los países donde se emitiría el voto.
Establecimiento de medios técnicos para garantizar la personalidad del votante y que el sufragio sea emitido sin coacciones ni influencias indebidas.
Un sistema riguroso de control y fiscalización técnica, realizado por agentes distintos a los que prestan el servicio.
Medios para garantizar el anonimato y el secreto del voto, separando cada voto de su emisor concreto (desconexión entre elector identificado y sentido del voto).

Estos requisitos técnicos han sido objeto de un análisis crítico reciente, Un análisis crítico y técnico de las recomendaciones emitidas por la OSCE/ODIHR sobre el voto por Internet (i-voting) en Estonia, nos sirve para profundizar en los desafíos técnicos, la implementación de estándares de seguridad y la gestión de la confianza pública. La adición de esta perspectiva técnica plantea preguntas clave sobre la *viabilidad* de los estándares al cuestionar su Implementabilidad, tanto desde la perspectiva técnica como legal, más allá de diseños sobre el papel. Se señala que si una recomendación es imposible de implementar, el fracaso en cumplirla puede ser utilizado por actores políticamente motivados para difundir la desconfianza en el sistema electoral. También se ha cuestionado que estos requisitos no suelen alinearse con las mejores Prácticas de otros sectores tecnológicos. Por ejemplo, se criticó la recomendación de evitar el mantenimiento diario de los servidores de votación por Internet, ya que esto violaría las mejores prácticas de funcionamiento de los sistemas de TI, a pesar de que el objetivo era la seguridad. Por último, las críticas se centran en la gestión de Críticas Políticas, recomendando que ODIHR no emita recomendaciones imposibles de cumplir, como la de abordar *proactivamente y a tiempo* todas las preocupaciones planteadas por las partes interesadas que desconfían de los resultados, especialmente cuando el objetivo de los críticos es la suspensión total del voto por Internet.

En resumen, aunque el voto por internet no está descartado como método viable, subsisten interrogantes técnicos y legales. Los estándares buscan conjurar las desventajas, como la posibilidad de ataques externos (hackers) o la manipulación interna. Una desventaja destacada es que la votación telemática puede socavar la transparencia y la universalidad del sufragio, ya que el cuerpo electoral puede perder el control del procedimiento, que pasa a ser monopolizado por expertos informáticos, lo que implica una cierta privatización del proceso. Solo presuponiendo una seguridad en el sistema técnico cabe imaginar su viabilidad constitucional.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

En esencia, el estándar internacional exige que el voto telemático debe ser equivalente al voto presencial para asegurar la igualdad del sufragio.

5.2 Casos de uso

5.2.1 Estonia: un caso de éxito

Estonia ha permitido el voto electrónico en remoto desde 2005 para las elecciones nacionales, municipales y del Parlamento Europeo. Es el caso más conocido de éxito del uso de internet para votar en remoto. Y además se trata de un sistema extremadamente abierto, que permite votar desde cualquier ordenador conectado a internet en cualquier lugar del mundo. Puede además decirse que el resultado ha sido satisfactorio. En las elecciones europeas de 2019 casi la mitad de los sufragios fueron remotos. Y en las nacionales de 2023 el porcentaje llegó al 60%, aunque descendió a un 40% en las europeas de 2024.

Estonia es un país con un sistema electoral proporcional, en el que los votantes deciden sobre listas abiertas de candidatos. Los electores pueden elegir votar en papel según el método tradicional sin necesidad de registro previo. También es posible votar en papel en el extranjero a través de las representaciones diplomáticas. Y como sucede en otros lugares, los votantes con necesidades especiales pueden solicitar que las urnas les sean llevadas a sus casas.

Pero lo diferencial es la votación remota a través de internet. Esta se realiza en un período previo al del día de las elecciones, concretamente entre el décimo y el cuarto día anteriores al domingo en el que se celebra la elección. Los votantes tienen que descargar en su ordenador una aplicación, en la que se identifican con la tarjeta física en la que llevan el ID de Estonia o con el ID oficial de su dispositivo móvil. Una vez autenticados, eligen los candidatos en la aplicación y confirman el voto con una firma electrónica. Pueden cambiar el voto durante todo el período de la votación remota, de modo que cada voto anula el anterior. Desde 2021, pueden también votar posteriormente de manera tradicional en papel el día de la elección. Este voto anulará el voto remoto hecho a través de internet. Se utiliza este mecanismo como

una protección adicional del secreto del voto, ya que la coacción que hubiera podido sufrir el votante podría ser corregida posteriormente (Ehin et al., 2022)

El sistema ha podido desarrollarse con eficacia gracias a la amplia implantación del ID estatal, obligatorio para todos los estonios y residentes permanentes en el país que sean ciudadanos de la UE. El ID está dotado de certificado digital y es ampliamente usado en todo el país para todo tipo de trámites. También se usa ampliamente el ID móvil (Parsovs, 2020)

Obviamente, esos certificados son usados a diario por la mayoría de la población porque la confianza en su seguridad es muy alta. Incluso a pesar de alguna crisis puntual, como la que llevó a la autoridad emisora a reconocer una vulnerabilidad en los IDs en 2017 que fue rápidamente corregida, el índice de confianza en la seguridad del sistema se acerca al 90% (Ehin et al., 2022)

El gobierno estonio ha puesto un gran interés en acreditar la solvencia del sistema. Desde su puesta en marcha, ha invitado a un grupo de expertos de la OSCE a actuar como observadores en todas las elecciones estatales celebradas con voto electrónico remoto. En general, salvo en el primer informe de 2007, las conclusiones han sido muy positivas.

Sobre la constitucionalidad del proceso, el Tribunal Supremo de Estonia se ha pronunciado en varias ocasiones (2011, 2013 y 2017) en sentido también confirmatorio, aunque en 2019 (Tribunal Supremo de Estonia 5-19-18, de 27 de marzo) estableció la necesidad de que algunos detalles del proceso que estaban regulados reglamentariamente fueran incorporados a la ley electoral.

5.2.2 El caso de México, del voto electrónico al voto remoto (VPI)

El voto por internet en México responde a una necesidad, la de satisfacer los derechos políticos de los millones de mexicanos residentes en el extranjero. Tras años de estudio, entre los que podemos destacar el trabajo realizado en 2013 por el Comité Técnico de especialistas para elaborar un análisis jurídico, técnico,

organizativo y presupuestal de las alternativas sobre el voto de los mexicanos residentes en el extranjero, en 2024 el voto por internet se planteó como una forma de voto complementaria al voto presencial, desarrollado en Embajadas y Consultados, como una forma de extensión de derechos.

Su validez había sido establecida jurisprudencialmente por el TEPJF, primando la ampliación de la participación, aunque algunas críticas señalan que el órgano judicial omitió la adecuada ponderación de principios frente a la pérdida de publicidad y el riesgo de coerción. La SUP-JRC-306/2011 es la resolución que abrió la puerta al voto por internet en México. De ella se dedujo la tesis XXIV/2012, que establecía que el voto por internet podría implementarse en las condiciones que se señalaban. En ese momento no existía el VPI a nivel federal, pero el Instituto Electoral del Distrito Federal (IEDF) intentó implementarlo para la elección de Jefe de Gobierno del DF. El Tribunal Electoral del Distrito Federal (TEDF) revocó la implementación del voto por internet argumentando que el sistema no garantizaba la certeza ni el secreto del voto. La Sala Superior revocó la decisión del tribunal local. Los magistrados determinaron que el sistema propuesto por el IEDF sí era válido y constitucionalmente viable, afirmando que la falta de una regulación legal exhaustiva no impedía el uso de tecnología si se demostraban medidas de seguridad razonables (auditorías, llaves criptográficas) que maximizaran el derecho al voto de los residentes en el extranjero sin sacrificar la certeza. El fundamento jurídico (artículo 343 de la LGIPE) exige que el sistema sea auditable, que permita al votante corroborar el sentido de su voto, que evite la coacción, garantice que solo el ciudadano con derecho vote, que evite el voto múltiple y que cuente con un programa de resultados en tiempo real.

Desde entonces el voto por internet ha sido clave para el Voto de los Mexicanos Residentes en el Extranjero (VMRE). Sin embargo no ha estado exento de problemas. En 2021 una auditoria de la ASF que fiscalizaba el contrato de Servicios para la infraestructura del sistema del VPI concluyó que el sistema, que utilizaron 12456 votantes, no cumplió con las características de un *Software como Servicio*

(SaaS). El sistema, diseñado y construido a la medida de los requerimientos del INE, no fue una aplicación disponible en la nube.

Durante el Proceso Electoral 2023-2024 la cifra de votantes, utilizando este sistema aumentó hasta los 160.181 votos (el 68% de los emitidos en el extranjero). Los pasos para su ejercicio eran simples: ingresar al SIVEI con la cuenta de acceso que recibirán al correo que hayan registrado al momento de inscribirse; completar el proceso de verificación siguiendo las indicaciones en el sistema y generar una contraseña; acceder al apartado de votación, marcar las boletas en las que tienen derecho a participar y confirmar el sentido de su voto para proceder con su envío. Una vez emitido el voto, se encriptó transfiriendose hasta un servidor de seguridad instalado en la Ciudad de México, por medio de tecnología *blockchain*, lo que permitió tener trazabilidad absoluta y evitar que cualquier sufragio pueda ser modificado en el trayecto. El sistema demostró su seguridad y su secreto, al no permitir vincular el sentido del sufragio con el votante. De esta manera se abría la puerta a un sistema de voto que, de mantenerse en el tiempo, permitirá que los mexicanos que han tenido que abandonar su patria se sigan sintiendo dueños de su democracia.

La experiencia mexicana con el voto electrónico, en ambas modalidades, demuestra un compromiso con la modernización de los comicios, evidenciado en la alta preferencia por el VPI (68% del total de votos en 2024) entre los mexicanos en el extranjero. El VPI, aunque esencial para garantizar la universalidad del sufragio para el VMRE, introduce un debate crucial sobre la legitimidad y seguridad del proceso. Los riesgos de manipulación invisible y el dilema irresoluble entre secrecía e integridad obligan a la ciudadanía a un "acto de fe". La falta de transparencia en las auditorías y el enfoque limitado en el riesgo crítico, en lugar de la funcionalidad, refuerzan la lógica de "seguridad por oscuridad".

La propuesta de extender el VPI al electorado residente en México carece de la justificación constitucional más sólida que esgrimió el TEPJF para el voto extranjero (la universalidad del sufragio) y cualquier avance debe ponderar rigurosamente la

conveniencia y legitimidad de su aplicación generalizada ya que aumentaría la probabilidad de coacción y violación del secreto aumentaría considerablemente.

En última instancia, el desafío para el INE y el sistema electoral mexicano es similar al que llevó al Tribunal Constitucional Federal de Alemania a prohibir el e-voto en su país: asegurar que la elección sea realizada "ante los ojos del público", permitiendo que cualquier ciudadano, sin conocimientos técnicos especializados, pueda comprender y controlar los pasos esenciales del proceso y el recuento. La velocidad de la tecnología no debe sustituir la necesidad de una democracia auditada y transparente.

5.2.3 Francia.

Si el voto electrónico presencial está estancado en Francia, el voto por internet ha consolidado su posición, pero exclusivamente para un cuerpo electoral específico: los ciudadanos franceses residentes en el extranjero. Regulado por los artículos R.176-3 y siguientes del Código Electoral, esta modalidad se permite para para la elección de diputados por los franceses residentes fuera de Francia

El protocolo se basa en varios roles clave, similares a los sistemas criptográficos de vanguardia (Debant 2023)

1. Servidor de Votación: Operado por el Ministerio de Asuntos Exteriores y Europeos, encargado de autenticar a los votantes y recolectar las papeletas.
2. Dispositivo de Votación: Un programa JavaScript que se ejecuta en el navegador del votante para crear y emitir el voto.
3. Autoridades de Descifrado: Dieciséis autoridades (ocho parejas de titulares/suplentes) que poseen una parte de una clave de descifrado, utilizando un esquema de umbral 4-de-N (se requieren al menos cuatro autoridades para descifrar).

4. Tercero Independiente: Un servidor externo operado por investigadores franceses (LORIA, CNRS, INRIA), encargado de proporcionar servicios de verificación para garantizar la integridad de la elección

Ya se ha mencionado en este trabajo la postura adoptada por la jurisprudencia ante las impugnaciones del voto electrónico presencial en Francia. Algo muy similar ha sucedido con las que se referían al voto por internet. Tras las elecciones legislativas de 2012 para los franceses en el extranjero, el Consejo Constitucional desestimó varias impugnaciones relacionadas con la modalidad electrónica. En algunos casos se volvía a confiar en las homologaciones técnicas. También se añadió la consideración de que los problemas no fueran cuantitativamente significativos (por ejemplo en la Decision n° 2012-4580/4624 de 15 febrero de 2013) También se repitieron las críticas a la "prueba imposible" pedida por los jueces en el sentido de una prueba de la alteración de los resultados (Guglielmi 2017) Algunos investigadores han afirmado haber encontrado vulnerabilidades críticas, aunque eso no les permita probar la alteración de los resultados (Debant 2023)

En cualquier caso, estas dudas no han desincentivado la participación. En las elecciones de 2024, en la segunda vuelta, podían votar más de un millón y medio de franceses residentes en el extranjero. Medio millón ejercieron su derecho. Y de esos, un 77% optó por el voto por internet frente a la opción de las urnas consulares o el voto por correo postal. Así que puede considerarse un modelo de éxito.

6 ¿La solución *blockchain*?

Frente a todos estos retos la introducción de *blockchain* sigue sin evitar el gran reto del voto digital de conjugar la seguridad y el anonimato que tradicionalmente se ha considerado un elemento básico del voto y las soluciones para hacerlo. Si mantener

la integridad de un sistema de votación basado en *blockchain* es razonablemente sencillo otros aspectos de implementar una arquitectura peer-to-peer de voto, como lograr mayor facilidad de uso y explicabilidad puede resultar más difícil. Según las objeciones planteadas, podemos decir que *blockchain* corre el peligro de ser la respuesta incorrecta ante algunos problemas de votación, como la necesidad de un voto secreto, verificable solo por el votante y por quien realiza el recuento, con posibilidad de probar que ha sido tomado en cuenta y realizado por la persona con derecho para ello (*trustable remote client*). Por eso, a pesar de los avances, la aplicación de *blockchain* al procedimiento electoral tiene que someterse a nuevas pruebas, ofrecerse en un modelo de negocio con un coste razonable y escalable y, para lograrlo, además del desarrollo tecnológico, el apoyo político será fundamental.

6.1 Un modelo de votación

La investigación sobre el uso de *blockchain* en el gobierno surgió en 2015 y, desde 2017 el interés en este tema ha aumentado drásticamente. Como se señaló, la tecnología basada en *blockchain* puede mejorar las formas en que se gestionan los datos gubernamentales específicamente al eliminar la participación de terceros. Por lo tanto, puede reducir las posibilidades de comportamiento corrupto. Esto es relevante también para el dominio de las elecciones y los sistemas de votación (Baudier et al., 2021).

Si tuviéramos que establecer un sistema estándar de votación a través de *blockchain* podríamos hablar del siguiente proceso: El registro de una dirección bitcoin ante la autoridad electoral. Esta lista sería publicada sin vincular la dirección con su propietario. Los candidatos publicarían su propia dirección. Los votantes emitirían su voto enviando una cantidad establecida al candidato elegido, lo que generaría un archivo que podría ser objeto de revisión.

Los partidarios de este sistema señalan como gran fortaleza su carácter descentralizado, lo que lo blindaría ante posibles alteraciones y manipulaciones. Entre las debilidades estaría la posibilidad de romper el secreto por parte de la autoridad electoral, que tiene el archivo que vincularía a los votantes con sus direcciones de bitcoin. Esto se podría resolver con un sistema de firma digital ciega, que permitiría a la autoridad electoral tener certeza de la emisión del voto sin vincular a cada votante concreto con el sentido del mismo.

Este sistema permite un seguimiento en tiempo real por parte de los candidatos y los mismos votantes (ilegales en prácticamente la totalidad de los sistemas electoral por su posible influencia en el voto), pero que abriría la puerta a posibilidades como que el elector pudiese cambiar el voto, en función de los avances en el resultado (teniendo validez sólo el último emitido). Pero para evitar este peligro se pueden establecer sistemas de votación a través de mensajes encriptados que sólo se podrían desencriptar finalizada la votación.

El archivo de esta información se realizaría siguiendo el sistema del *bulletin board* (Benaloh y Tuinistra, 1995), que podría establecerse en una sencilla página web por parte de la autoridad electoral. Esta fórmula otorga a la autoridad electoral capacidad de manipulación de la información ofrecida, lo que si bien puede ser detectable a priori no serviría para prevenir las alteraciones sino para detectarlas y denunciarlas a posteriori. Optar por mecanismos de *blockchain* evitaría esta función de filtro, eliminando posibilidades de censura. Una vez introducido nadie puede modificarlo y todos tienen acceso a la misma información.

El concepto de identidad soberana propia (SSI, por sus siglas en inglés) es otro posible sistema de gestión de identidad que se puede utilizar en un sistema de votación electrónica centrado en el control del usuario. El SSI se basa en las cadenas de claves criptográficas compatibles con *blockchain*. En el corazón de SSI se encuentra el estándar de identificador descentralizado (DID). DID es una identidad

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

que conecta el documento DID con datos relacionados con claves públicas autorizadas para este DID y puntos finales de servicio necesarios para realizar una conexión (Schäffner, n.d.). El SSI funciona como "un sistema de gestión de identidades creado para operar independientemente de actores públicos o privados de terceros, basado en arquitecturas tecnológicas descentralizadas y diseñado para priorizar la seguridad del usuario, la privacidad, la autonomía individual y el autoempoderamiento" (Giannopoulou & Wang, 2021) . El potencial de SSI también se destaca con respecto a los servicios públicos. La Generalitat de Catalunya en España presentó al público un novedoso modelo de identidad digital descentralizado y auto-soberano conocido como Identicat. Este modelo promete ser autogestionado por el ciudadano con garantía jurídica y validez para ser explotado tanto en dominios públicos como privados (Gencat, 2019).

6.2 Una visión crítica

Los más críticos, por su parte, creen que la utilización de la tecnología *blockchain* traerá consigo más problemas que soluciones, al introducir nuevas vulnerabilidades que no existían antes, sin ofrecer soluciones claras para los problemas de fondo que plantea el voto online. Estas nuevas vulnerabilidades, supondrían un problema mayor que los que trataría de resolver (Blaze, 2017). Para estos críticos la vulnerabilidad de los registros, a los que *blockchain* ofrece solución, no son la principal debilidad del voto electrónico sino la imposibilidad de garantizar la libre emisión del voto. La actualización de los censos es hoy una tarea permanente, y generar o distribuir identidades, protegerlas del robo, revocar o gestionar autorizaciones pérdidas, y demostrar la identidad o la propiedad de las claves en el momento de votar, son cargas que el sistema hoy no puede soportar. Muchos de estos problemas podrían solucionarse pero para hacerlo existe un obstáculo: la necesidad de mantener la universalidad del voto, su ejercicio accesible para todo el mundo, más allá de *frikys* tecnológicos o *early adopters*.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Los críticos ni siquiera aceptan como argumento la que sería la principal fortaleza de la tecnología de cadena de bloques, que ha convencido a muchos de su contribución a la mejora de los procedimientos electorales: la inmutabilidad de sus datos por lo que una vez que las transacciones (en este caso los votos) se registran en la red, no pueden ser modificadas[3]. En su opinión, es cierto que la manipulación de estos datos es la principal amenaza de los procesos electorales, en especial cuando se trata de procesos automatizados, cuya vulnerabilidad ha quedado en evidencia en casos como el simulacro de votaciones web en Washington DC, en el año 2010. El uso de *hash chains* permite conservar los registros conservando su anonimato mientras se abre el sistema a auditorías externas, construyendo auténticas urnas digitales y generando informes con las evidencias sobre la integridad de la elección. *Blockchain* ofrece posibilidades en este sentido, para registrar información crítica de la elección (votos emitidos y nulos, si un votante ha votado efectivamente o no, etc.). El mecanismo utilizado para su funcionamiento requiere un consenso sobre los eventos y su orden, y una vez que estos se introducen en una urna encriptada pasan a formar parte de la cadena de bloques en la que no pueden ser ni modificados ni reorganizados respecto al resto. Hacerlo requeriría de un compromiso de todas las partes para alterar las normas, algo estadísticamente imposible, garantizando así la integridad de esta parte del proceso. En cualquier momento es deseable que los nodos de la red, alimentados por la autoridad electoral y organizaciones políticas – que deberían alojarse en sistemas confiables y fácilmente auditables- adquirirá un peso en el sistema que sobrepasará el de los votantes individuales, incluso, cuando existieran intentos de alterar el mecanismo podrían detectar estos ataques (tanto por las organizaciones, el resto de la red, como por observadores externos) y tratar de solucionarlo.

Una arquitectura *peer-to-peer* plantea dudas sobre la seguridad, distintas de las que hasta ahora se planteaban en el voto electrónico. Si un sistema controlado por la autoridad electoral ofrece vulnerabilidades vinculadas a esta autoridad central, un sistema construido sobre estructuras individuales o de organizaciones políticas,

abriría muchas otras vulnerabilidades. Es imposible construir un sistema entre pares (P2P) E2E-VIV, utilizando solo nodos 100% confiables. De ahí la necesidad de concentrar los esfuerzos en asegurar que ningún elemento corrupto, o un grupo de ellos, pueda comprometer los resultados sin ser detectado, violar la privacidad de los votantes o los requisitos que hacen los sistemas E2E-VIV recomendables. De esta forma, algunos advierten esta inmutabilidad como una de sus principales debilidades, al considerar que es imposible mantener la seguridad de esta información, y considerar que esto pondría en grave riesgo una información privada altamente sensible.

Para evitar estos peligros se plantean alternativas hibridas, que buscan solucionar esta debilidad a través de la centralización del proceso en una autoridad electoral. En este sistema alternativo los votos son enviados desde distintos dispositivos a una autoridad electoral, y contabilizados en un formato encriptado. El votante puede utilizar su clave para comprobar que su voto fue procesado adecuadamente, lo que reduciría el riesgo, pero no lo anularía como sostienen algunos que lo consideran, además, un riesgo para el secreto del mismo (Torres, 2022). Proteger del hackeo a los dispositivos conectados, es tan difícil que aunque se consiguiera desarrollar un sistema online de voto que mantenga todos los atributos necesarios para que existan elecciones democráticas sería increíblemente difícil de lograr la seguridad absoluta, algo que según los expertos no existe.

Ante la crisis de credibilidad, la apuesta de *blockchain* es que cada vez sea menos necesario confiar y más sencillo verificar. Para lograrlo nos enfrentamos al dilema de reforzar el control del Estado para garantizar la integridad del proceso electoral o buscar nuevos caminos, utilizando la tecnología *blockchain*, para abrir y distribuir entre los ciudadanos el control de los sistemas de votación. Otra decisión importante es si utilizar cadenas de bloques públicas y abiertas o cadenas privadas y con autorización.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

El elector debe ser plenamente identificado para demostrar que está habilitado para votar y que no votará más de una vez; pero al mismo tiempo se le debe garantizar la privacidad necesaria para que su voto sea anónimo. Construir un sistema en el mundo digital que cumpla estas premisas, parece una tarea cuesta arriba, aun contando con una tecnología como blockchain. El sistema, sigue enfrentándose al gran reto del voto digital de conjugar la seguridad y el anonimato que tradicionalmente se ha considerado un elemento básico del voto y las soluciones para hacerlo, se fundamentan en la existencia de sistemas sólidos de identidad digital. Para garantizar el secreto, algunos países exigen requisitos legales como que se vote individualmente, asegurándose que no hay nadie mirando y añadiendo una declaración solemne de que el voto fue decidido personalmente (Tribunal Constitucional Alemán). Estos requisitos del voto postal deberían ser aplicables al voto electrónico, especialmente para prevenir la manipulación de la información, proteger el anonimato y mantener la autenticidad y la integridad de los votos.

Resumiendo, si mantener la integridad de un sistema de votación basado en *blockchain* es razonablemente sencillo en un sistema E2E-VIV, otros aspectos de implementar una arquitectura peer-to-peer de voto como la distribución de los terminales "clientes" a votantes y organizaciones o lograr mayor facilidad de uso y rendimiento, etc. puede resultar más difícil. Según las objeciones planteadas, podemos decir que *blockchain* corre el peligro de ser la respuesta incorrecta ante algunos problemas de votación, como la necesidad de un voto secreto, verificable solo por el votante y por quien realiza el recuento, con posibilidad de probar que ha sido tomado en cuenta y realizado por la persona con derecho para ello (*trustable remote client*).

No podemos pensar en *blockchain* como un sistema electoral en sí mismo, sino como un mecanismo que nos puede ayudar a solucionar algunos de los problemas existentes. La integridad de una elección requiere el derecho de sufragio pasivo, el sufragio universal, la garantía de una serie de derechos fundamentales con efectos

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

electorales como la libertad de información de asamblea y de asociación, y un voto directo, igual, secreto y libre.

La aplicación de *blockchain* al procedimiento electoral tiene que someterse a nuevas pruebas, ofrecerse en un modelo de negocio con un coste razonable y escalable y, para lograrlo, además del desarrollo tecnológico, el apoyo político será fundamental. A continuación vamos a analizar el desarrollo de distintas plataformas de votación y la puesta en práctica de alguna de ellas alrededor del mundo. Sus resultados nos permiten contemplar con esperanza sobre las posibilidades de consolidar prácticas basadas o apoyadas en *blockchain* dentro de los procedimientos electorales.

6.3. Plataformas de votación basadas en *blockchain*

Una visión general nos permite localizar por todo el mundo plataformas de voto electrónico, donde es posible encontrar distintas propuestas con tecnología *blockchain* como Democracy Earth Foundation, Follow My Vote, democracyos.org, VoteWatcher, Milvum, VotoSocial, Coinstrack, Bobak, Secure Vote, *blockchain* Technologies Corp., E-Vox, Swarm, Boatz, Boule, Ballotchain, BitCongress, Polys y *blockchain* Voting Machine, Chaintegrity. Aunque por lo general no hay grandes diferencias entre ellas, a continuación, nos detendremos en las más novedosas.

Unos de los primeros proyectos en aplicar la contabilidad distribuida en las votaciones fue Polys[5], desarrollada por la incubadora Kapersky Lab y basada en los contratos inteligentes de Ethereum. La peculiaridad de esta plataforma es que no funciona completamente con la cadena de bloques tradicional de Ethereum, sino que realiza los cálculos de las votaciones encriptados para asegurar el anonimato del voto. A pesar de la encriptación de los cálculos, el monitoreo y la auditoría son sencillos y rápidos. Se trata de una plataforma gratuita y modificable, en la que algunas funciones son de pago.

Otro modelo es el de Coinstack v3.0, desarrollada por la empresa Blocko, y que ha recibido la certificación de calidad internacional que otorga el gobierno de Corea del Sur. La plataforma está construida de forma tal que los desarrolladores puedan elaborar sus propias aplicaciones *blockchain* con las múltiples opciones que ofrece el SDK (kit de desarrollo de software) y las API (interfaz de programación de aplicaciones). Además, Coinstack funciona en la *blockchain* de Bitcoiny es, también, compatible con los contratos inteligentes de Ethereum, lo que permite la creación de una red *blockchain* propia de "forma segura y transparente". Esta plataforma fue la utilizada en el proyecto de la provincia surcoreana de Gyeonggi-do para elegir entre varias propuestas de las que hablaremos más adelante.

Bobak, desarrollada por la startup británica Monax, unida al proyecto Hyperledger, que plantea un sistema de votaciones descentralizadas "multijurisdiccional" basada en Etherum, brinda acceso a los participantes de diferentes países a través de la creación de un contrato inteligente (un acuerdo entre partes que, en el momento que se cumplen las condiciones pactadas, se autoejecuta, conocido por su denominación en inglés "*smart contract*"). El sistema requiere de la participación de los organismos oficiales, que deberían publicar un contrato inteligente. En él se establecerían las jurisdicciones en las que se realiza la votación y el registro de quienes serán los votantes, que se registrarían a través de una web encriptada. El registro contará con dos factores de verificación que se realizarán en persona, en las oficinas del gobierno local. El tercer paso ocurrirá cuando los votantes accedan a la plataforma descentralizada, que estará alojada principalmente en los servidores Monax en los Alpes suizos. Allí, podrán depositar el homólogo de la papeleta de votación, pero digital y dentro de la cadena de bloques de la startup británica. Este sistema ofrece un extra de seguridad añadiendo a la descentralización de la información propia de *blockchain*, una copia de seguridad en los servidores de la *startup,* creando, además, un mecanismo de votación basado en *blockchain* y la teoría del juego de Schelling, también conocida como *Schelling point*. Ya se ha

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
red.es
Plan de Recuperación, Transformación y Resiliencia

realizado algunas experiencias, por ejemplo, en la ciudad alemana de Bielefeld y en la ciudad estadounidense de Punxsutawney, Pensilvania.

Secure vote, es otra alternativa para la votación enfocada en la transparencia y la eficacia de la *blockchain* de Bitcoin. Secure vote fue desarrollada por la startup australiana XO.1, y permite las votaciones tanto en dispositivos móviles como en máquinas de votación conectadas a la red. En este caso, lo relevante es la escalabilidad, otra de las críticas habituales de estos sistemas, y que la plataforma afrontó a través de una prueba de estrés de 1.500 millones de votos verificados en la cadena de bloques, en la que el problema principal fue el retraso en las transacciones de una media hora. Un retraso razonable si tenemos en cuenta que el número de votos supone 1/5 de la población mundial.

Voatz, que también forma parte de Hyperledger Project, combina la tecnología *blockchain* con la biométria, enfocándose en la identidad, otra de las debilidades habituales de estos sistemas, para autenticar la identidad del votante. Voatz ha sido utilizado en Estados Unidos en elecciones a colegios, sindicatos, ONG's, y también fue utilizada para autentificar las acreditaciones de los delegados de la Convención Demócrata en 2016 y por el Senado de Virginia Occidental.

Boule es otra plataforma de voto basada en Ethereum. Los organizadores de procesos electorales deberán adquirir tokens para activar un contrato inteligente específico para la celebración de elecciones, desarrollado por la Fundación Boule. El sistema utiliza una identificación basada en ID y reconocimiento facial para la emisión del voto, encriptando los votos emitidos de una forma que, según la plataforma, hace imposible tanto la manipulación de los resultados como romper el anonimato del voto.

E-vox es un sistema basado en Ethereum y contratos inteligentes que se integraría en las plataformas electorales ya existentes, como el sistema de epeticiones, que

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

comenzarían a migrar a *blockchain*. El sistema que tendría una aplicación electoral y formato móvil integraría distintos tipos de verificación de identidad, en función del tipo de votación, desde el teléfono móvil para las peticiones, al BankIDs (gestionado por los tres bancos más grandes de Ucrania) para las votaciones. Además se utilizarían los cajeros electrónicos como lugar de votación.

Con respecto a desarrollos más recientes, Zhang et al. (2020) propuso un novedoso sistema BEV, denominado Chaintegrity. Sus desarrolladores crearon un marco que consta de nueve requisitos críticos que deben cumplir los sistemas BEV actuales. La escalabilidad, la mejora de la privacidad, la verificabilidad universal, la verificabilidad de extremo a extremo, la posibilidad de votar y continuar, la no reutilización, la asequibilidad, la equidad y la solidez, según su evaluación, mucho de estos no se garantizarían en los sistemas de votación basados en *blockchain* como Agora, Follow my Vote, TIVI, VYV o SHARVOT. Del mismo modo, Baranski et al. (2020) propuso un sistema de voto electrónico que preserva la privacidad basado en la red pública Stellar *blockchain* que cumpliría con los requisitos obligatorios.

6.4. Experiencias

Las posibilidades de aplicar *blockchain* a los sistemas de votación, se comenzaron a explorar en Dinamarca en 2014, en las elecciones internas de the Liberty Alliance, donde utilizaron este Sistema de registro distribuido para su convención anual. En la misma época el Republican Party of Utah también utilizó *blockchain* en sus votaciones primarias para la elección del candidato presidencial, en las que se registraron para votar a través de este sistema unos 59.000 ciudadanos, que debían inscribirse previamente en la plataforma utilizada Smartmatic. En la misma línea, en 2016, el Partido Libertario de Estados Unidos (*US Libertarian Party*) utilizó este sistema en elecciones internas en Texas, en el que participaron 250 personas, tanto para el registro como para el recuento. En la base de cada urna se pusieron 3 códigos QR que contenían la dirección de *blockchain*, la identificación de la urna y el

voting ID. Tras escanear los códigos los datos se incluían en *blockchain* para evitar el fraude. Esta tecnología también fue utilizada para autentificar las acreditaciones de los delegados de la Convención Demócrata en 2016.

Más allá de los partidos políticos, en Estados Unidos, el Estado de Maine y el de West Virginia han comenzado a estudiar y desarrollar sistemas de votación basados en *blockchain*. En el Estado de Maine (EE. UU.) en 2017 se planteó la creación de una comisión de estudio sobre el tema, con el propósito de explorar las posibilidades de utilizar *blockchain* en las elecciones del Estado, pero esta fue rechazada por los legisladores. En West Virginia el voto se realiza a través de una aplicación móvil, dentro de un Proyecto piloto dirigido a militares destinados fuera de Estados Unidos. Este proyecto, que ha sufrido todo tipo de advertencias sobre sus posibles vulnerabilidades, ha apostado por el *blockchain* para afrontar esos riesgos. La aplicación fue desarrollada por Voatz, y durante las primarias se puso en marcha para los votantes registrados en dos condados del Estado, que se encontraran fuera de USA. Tras los resultados, las autoridades estatales han decidido ampliarlo a los votantes de todo el Estado. Para el sufragio descentralizado de personal militar destacado en el extranjero y otros estadounidenses autorizados para votar en el país en el que se encuentran. Los votantes solo requirieren de una identificación válida y un dispositivo móvil Android o Apple, lo que al no cumplir con el principio de neutralidad tecnológica, deja fuera a todos aquellos que utilicen otros sistemas operativos. El Sistema se basa en la autenticación biométrica y el registro de los votos en un *blockchain* privado. Para el proyecto piloto, han preparado 8 nodos verificados (controlados todos ellos por la empresa) que comprueban algorítmicamente que los datos son válidos antes de añadirlos a la cadena. Es interesante reseñar que no estaríamos ante un sistema basado 100% en *blockchain* sino ante una aplicación móvil que tiene un *blockchain* adjunto. En este caso *blockchain* ni puede proteger la información desde su emisión ni garantiza que coincida con la voluntad del votante. Básicamente los problemas del voto online seguirían siendo los mismos.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
red.es
Plan de Recuperación, Transformación y Resiliencia

En Corea del Sur, la experiencia se realizó en la provincia de Gyeonggi-do, con la participación de unos 9.000 residentesy sobre el Proyecto de Apoyo a la Comunidad Ddabok. La votación, que sirvió para seleccionar proyectos de ayuda comunitaria entre los presentados por los residentes, se basó en el uso de contratos inteligentes para garantizar la transparencia y evitar la manipulación de los datos. En este caso, la consulta fue vinculante y sirvió para seleccionar más de 500 proyectos comunitarios.

En Australia, en 2016, la compañía pública de correo comenzó a desarrollar un sistema de voto escalable que empezaría con pequeñas elecciones locales para terminar aplicándose en las elecciones parlamentarias.

La ciudad de Zug, en Suiza, también ha realizado ya una primera prueba de sistema de votación sustentado en *blockchain*, desarrollada conjuntamente con la Universidad de Lucerna. El sistema, que prevén que tardará entre 5 y 10 años en estar en marcha con efectos vinculantes, se basa en la identidad digital construida por los ciudadanos a través de distintos procesos, como certificarse en universidades o manejar su cuenta bancaria, entre otros.

Japón es otro país del sudeste asiático que introdujo la votación digital *blockchain*. LayerX, una startup japonesa de *blockchain*, que se incorporó al sistema de votación como parte de la iniciativa de ciudad inteligente de Tsukuba (Das, 2018). En Tailandia, el Centro Nacional de Tecnología Electrónica e Informática (NECTEC) también ha estado desarrollando una plataforma de votación habilitada para *blockchain*. Esta plataforma permite que las personas usen el correo electrónico para votar mediante el reconocimiento facial de las cámaras de teléfonos o computadoras portátiles para verificar la identidad. Actualmente, NECTEC planea realizar su prueba entre expatriados que quieren votar en las elecciones nacionales (Vinnakota, 2021).

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Ucrania también ha trabajado en desarrollar un sistema de estas características basado en Ethereum y contratos inteligentes E-vox y comenzó a trabajar en otro proyecto de sistema de voto descentralizado basado en *blockchain* y contratos inteligentes, promovido por la autoridad nacional electoral, que utilizaba la plataforma NEM con 28 nodos, situados en las comisarías de policía.

También en las elecciones presidenciales, en Sierra Leona (2018) se anunció el uso de *blockchain* para las votaciones. El anuncio de la compañía Agora Voting, fue replicado por un buen número de medios de comunicación, obligando a la autoridad electoral de Sierra Leona a clarificar la situación, negando haber utilizado *blockchain*, ni los servicios de Agora Voting. Aunque la situación no llegó a clarificarse del todo, parece ser que se trataba de un experimento autorizado en 280 de los más de 11.000 colegios electorales, para, a través del contraste con los resultados del recuento manual, mostrar la fiabilidad del sistema[15].

En la misma línea, en España, se plantean dudas sobre si los organizadores de la consulta sobre la independencia de Cataluña recurrieron al *blockchain* para sortear algunas de las limitaciones técnicas establecidas por las autoridades españolas en los sitios web para garantizar la prohibición de celebrar un referéndum contrario a la legislación vigente en España. Aunque se ha señalado que ante la imposibilidad de recibir soporte de las autoridades electorales, se utilizó la tecnología *blockchain* para la activación del censo universal, recurriendo a tecnologías como tor, signal o bitcoin, no hay constancia de esta utilización y solo consta la publicación del censo en protocolo IPFS, permitiendo el acceso de manera distribuida sin depender de ningún servidor específico mediante conexiones usuario a usuario. Quizás por eso mismo el sistema mostró su vulnerabilidad, como consecuencia de la clave elegida para el descifrado de todos los datos que almacenaban en el IPF (1714, fecha de la derrota en Barcelona de los partidarios del archiduque Carlos frente a las tropas de Felipe V, que se conmemora como el Día de Cataluña) permitiendo acceso al

registro específico de un ciudadano y, por consiguiente, a sus datos personales, lo que ha generado un grave problema de privacidad para millones de electores.

La sociedad civil también ha comenzado a experimentar con estos sistemas. En Colombia se realizó una prueba piloto, en dos colegios de Bogotá, en la que participaron más de 1400 estudiantes, para elegir a sus representantes estudiantiles, desde una plataforma diseñada por el laboratorio de la Universidad Nacional de Colombia. A nivel nacional también la sociedad civil en Colombia se organizó, basado en *blockchain*, un simulacro de votación, el proyecto plebiscito digital, para facilitar a los expatriados el voto en el plebiscito sobre los acuerdos de paz de 2016. Algo que también ocurrió en México, promovido por organizaciones de la sociedad civil que han empezado a promover este tipo de votaciones. La ONG República Cero celebró un simulacro de elección presidencial, ebm2018.org. Otro grupo de estudiantes mexicanos agrupados en torno a ElectChain, desarrollaron una aplicación para móviles y navegadores basada en *blockchain*, a través de la cual generaron un proceso electoral alternativo, no oficial. La plataforma Voatz, ha sido utilizada en Estados Unidos en elecciones a colegios, sindicatos y ONG's.

En España, las votaciones basadas en *blockchain* se han empezado a usar en el ámbito privado para determinadas juntas de accionistas como la del Banco de Santander, que buscaba "la transparencia del voto por delegación de los inversores institucionales ("proxy voting") así como aumentar la eficacia operacional, la seguridad y el análisis". El sistema fue desarrollado por Broadridge, en colaboración con JP Morgan y Northern Trust, en la plataforma de *blockchain* Quorum. Un requisito, el de confirmar los votos a los inversores finales, que será obligatorio tras la entrada en vigor de la Directiva Europea sobre Derechos de los Accionistas, en junio de 2019 y requerirá compartir información entre los intermediarios el mismo día hábil, algo para lo que el uso de *blockchain* puede marcar la diferencia.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial
red.es
Plan de Recuperación, Transformación y Resiliencia

En la capital rusa, Moscú, se lanzó un servicio de "Hogar digital" en 2018. Este servicio opera a través de la plataforma de voto electrónico Active Citizen y permite a los residentes de Moscú organizar reuniones y votar sobre diferentes temas de gestión de la casa (Kshetri & Voas, 2018). El gobierno de Moscú encargó a PwC que evaluara la eficiencia y la credibilidad del BEV. Según el informe, el sistema “ha demostrado ser gravemente vulnerable” (Park et al., 2021). Otros países como India están explorando las posibilidades de integrar la tecnología *blockchain*. La propuesta de IIT Madras, desarrollada junto a el Centro para el Desarrollo de Computación Avanzada (CDAC), ha cumplido con los criterios de la Comisión Electoral de India para integrar *blockchain* para el voto electrónico seguro (Agrawal et al., 2021).

6.5 Los obstáculos al uso de *blockchain* para las elecciones

No podemos terminar sin hacer mención a los debates que en la comunidad *blockchain* se están celebrando en torno a la gobernanza del instrumento, en el que se apunta un debate profundo sobre la propia naturaleza de la democracia. Como apunta Boucher, la extensión de *blockchain* en los procedimientos electorales, dependerá de su capacidad de reflejar los valores y estructuras de la sociedad, la política y la democracia (Boucher, 2017). De manera similar, Magnuson (2020) señala que considerar la tecnología *blockchain* como "salvadora o verdugo de la democracia" ensombrece un debate más crucial: "que muchos de los beneficios y peligros de *blockchain* reflejan los beneficios y peligros de la democracia" (p. 194-195).

De ahí que haya que prestar atención a los problemas que nos encontramos al describir la aplicación de *blockchain* en el procedimiento electoral y que guardan relación con lo inadecuado del instrumento para garantizar la emisión libre del voto.

7. CONCLUSIONES

El análisis realizado en estas páginas de la implantación y el desarrollo -incluidos los retrocesos- de los sistemas de votación electrónica en un número significativo de países permite esbozar un resumen de sus principales ventajas e inconvenientes.

7.1 Automatización y eficiencia de los procesos electorales

En principio, los sistemas de voto electrónico presentan importantes ventajas de automatización y eficiencia. Al no ser necesario elaborar, imprimir y procesar papeletas físicas se eliminan muchos de los costes de tiempo y de dinero asociados a las mismas. Por ejemplo, no son necesarios espacios de almacenamiento físico ni logística de transporte. Y los recursos humanos y materiales necesarios para gestionar el sistema tienden a ser mucho menores una vez se ha realizado la inversión tecnológica inicial.

Pero donde esta automatización impacta más decisivamente es en el momento del escrutinio. Los resultados -y el proceso de revisión de los mismos o de corrección de errores- pueden ser casi instantáneos. La rapidez en el recuento puede ser crítica en procesos electorales muy polarizados y eso puede marcar la diferencia entre la aceptación del resultado o su deslegitimación.

El sistema también presenta ventajas de eficacia ligadas a la escalabilidad y el uso del mismo software o las mismas máquinas en diferentes procesos electorales. También resulta más sencillo absorber un número de votantes superior al previsto, lo que es puede ser más complicado en un sistema de votación en papel tradicional.

Por supuesto, todas estos beneficios son aún mayores en los sistemas de voto electrónico remoto. En ellos, es el propio elector el que proporciona el hardware y el espacio en el que se realiza la votación. Desaparecen además los riesgos de que parte del material resulte dañado durante la jornada electoral como consecuencia de algún accidente o de los incidentes provocados que pudieran producirse durante la votación.

Como ya se ha adelantado, esta eficacia puede anularse cuando se producen errores técnicos graves en las fases iniciales de la implementación. El caso de Holanda y el de Valonia en Bélgica pueden ser buenos ejemplos. Los defectos del software o de las máquinas pueden provocar costosas sustituciones o impugnaciones de los recuentos que introducen nuevos plazos y retrasan los resultados definitivos.

No parece que haya recetas mágicas para asegurar desde el principio que los sistemas de voto electrónico sean de por sí mejores en el apartado de la eficacia y la automatización. Parece que si los electores confían en la autoridad electoral, tienen paciencia para esperar a la corrección de los errores. La otra alternativa es volver al voto tradicional cuando estos se presentan de modo traumático e inesperado.

7.2 Aumento de la participación

Sobre la participación, la valoración cambia de modo decisivo en función de que el voto electrónico sea remoto o presencial. Como hemos visto, los estudios realizados en países que han mantenido el voto tradicional y el electrónico presencial sugieren que la participación disminuye ligeramente en estos últimos. El dato no resulta sorprendente. Si es necesario acudir en cualquier caso al colegio electoral, es posible que la dificultad real o percibida del manejo de la tecnología pueda desincentivar el voto de algunas personas.

Por el contrario, parece claro que la participación aumenta cuando se implanta un sistema de votación electrónica en remoto, lo cual resulta bastante lógico. Y no solo se trata de la comodidad de votar desde cualquier lugar sin necesidad de desplazarse. También desaparece parte del miedo o la inseguridad que pueden asociarse al voto presencial en algunos lugares del mundo.

7.3 Seguridad

En principio, el voto electrónico presencial o remoto presenta también ventajas tecnológicas desde el punto de vista de la seguridad del proceso. Al hablar de

seguridad nos referimos a la capacidad de un sistema electrónico de proteger la información y de dejar trazas de todas las operaciones e intervenciones sin que estas puedan ser negadas por emisores o receptores (no repudio) y sin que los datos puedan ser alterados (integridad) Como hemos visto, los sistemas basados en *blockchain* presentan especiales ventajas en estos puntos.

Por otra parte, algunas de las crisis que han provocado la suspensión temporal o definitiva de estos sistemas han estado relacionadas justamente con la falta de seguridad. Así sucedió en parte en Bélgica y en Holanda y también en otros lugares.

También conviene notar que tan importante como la seguridad misma del proceso es la percepción de la misma por parte de los votantes y de los partidos políticos. Como veremos más adelante, la transparencia y explicabilidad de los procedimientos -especialmente de los de revisión- es más importante que la propia seguridad efectiva de los mismos.

7.4 Transparencia y explicabilidad

A la vista de las experiencias examinadas en estas páginas, la transparencia y/o explicabilidad del proceso parece ser el punto más crítico. Y en este punto es donde los sistemas de voto electrónico presentan su flanco más débil. Siempre parece más complejo explicar la tecnología que un sistema de papeletas impresas almacenadas en urnas. Y este problema se agudiza cuando se plantean dudas sobre la corrección del resultado. En el caso del voto tradicional, se pueden consultar las actas firmadas por las autoridades de las mesas y validadas por los representantes de los partidos. Y pueden cotejarse, normalmente, con las copias que estos representantes -o el público en general- se haya llevado consigo tras el escrutinio de los votos. En algunos casos, incluso, está prevista la posibilidad de abrir de nuevo las urnas y volver a contar los votos. Todo este procedimiento es lento y costoso pero resulta transparente y fácil de explicar.

En el caso del voto electrónico las cosas pueden ser percibidas de un modo muy diferente.

Cuando se trata de un voto electrónico presencial, parece que algunos de los sistemas utilizados son más transparentes o explicables que otros. El modelo belga, descrito aquí con cierto detalle, es un ejemplo de sistema sencillo, desconectado y razonablemente explicable.

En el voto electrónico remoto, sin embargo, el reto presenta dificultades que parecen difíciles de superar. Es prácticamente imposible que un votante entienda en rigor la garantía del encriptado criptográfico de una firma electrónica. Y lo mismo sucede con la trazabilidad de los datos o la integridad basada en una cadena de bloques. También en lo que respecta al secreto del voto, al que nos referiremos a continuación. La experiencia muestra que en los pocos casos de éxito -eminentemente el de Estonia- el soporte esencial es la confianza en las autoridades y el hábito de uso de esos certificados electrónicos o de los IDs digitales en otras operaciones administrativas de la vida ordinaria sin que se presenten problemas significativos. También incrementa esa confianza el recurso frecuente a auditorías externas independientes.

7.5 El secreto del voto

El procedimiento clásico para asegurar el secreto del voto son las cabinas electorales. Como es sabido, para que esto funcione bien es necesario que se cumplan una serie de requisitos anteriores y posteriores. En el momento de la votación, es necesario asegurar que el local electoral tiene unas cabinas lo suficientemente amplias como para contener las papeletas de todas las candidaturas y los sobres en los que estas han de ser introducidas. Además, el diseño de la cabina debe permitir que el elector quede libre de las miradas del resto de personas que se encuentren en el local. Es un procedimiento simple y una garantía fácil de comprender para los ciudadanos. Pero no está exento de problemas. Es necesario que esas condiciones se mantengan a lo largo de toda la jornada de votación. Y lo habitual es que en cualquier elección importante, con miles de locales, sucede que las papeletas se agotan o son sustraídas en algún momento

de la jornada. O que la cabina se deteriora y no se cumplen los requisitos de privacidad.

Pero obviamente, el secreto del voto en papel no se ve afectado solo por los inconvenientes de las cabinas electorales. La compra de votos es relativamente sencilla. Basta con entrar en el local con una papeleta que ha sido introducida en el sobre previamente -fuera del local- en presencia de la persona que ha pagado por el voto. Después, solo es necesario que alguien observe en el interior que el votante no altera la papeleta antes de depositarla en la urna. Para tratar de evitar esto, se puede obligar a todo el mundo a entrar en la cabina y permanecer en ella un tiempo mínimo para asegurar la privacidad. En la práctica, esto dificulta la fluidez del proceso y tampoco asegura que la compra no vaya a producirse. Es sencillo utilizar un dispositivo móvil para fotografiar o retransmitir en vídeo desde la cabina y demostrar así que se ha votado lo que estaba pactado.

Es interesante considerar estas cuestiones para abordar el secreto del voto electrónico con la perspectiva adecuada. No se trata de saber si puede garantizarse en términos absolutos, sino más bien si puede mejorar los defectos de un sistema de votación clásica en papel. Y no solo en un sentido objetivo o científico, sino sobre todo desde el punto de vista de la confianza que pueda generar en los votantes. Tendría poca eficacia una demostración técnicamente compleja de la garantía del secreto de voto en los sistemas electrónicos si no hubiera una forma de explicarla a los electores.

Cuando se habla del voto electrónico remoto, es frecuente plantear la paradoja de la amplia aceptación del uso de banca electrónica en remoto en contraste con la desconfianza que genera el uso electoral de técnicas parecidas. Pero suele obviarse una diferencia esencial entre ambos procedimientos: el secreto del voto. En la información bancaria no hay ningún inconveniente en que el banco sepa qué hacemos con nuestro dinero. Más bien al contrario, se trata de asegurar que el banco sepa exactamente qué es lo queremos hacer con nuestro dinero. Pero en el caso de la votación en remoto hay que jugar con un factor que complica

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

enormemente las cosas: el gestor del sistema tiene que permanecer ciego ante lo que ha votado el elector. Y eso no solo durante el acto de la votación sino también en el recuento posterior y en las impugnaciones o chequeos que hayan de realizarse.

Como hemos visto al tratar el caso belga, el secreto de voto parece alcanzable en un sistema de voto electrónico presencial con máquinas desconectadas y tarjetas de acceso sin identidad (ésta se acredita en la mesa) Pero resulta mucho más complejo en los sistemas remotos. Sobre la garantía del secreto en el voto electrónico en ellos no parece haber un consenso claro. De hecho, es amplio el número de autores que consideran incompatible el secreto de sufragio y los sistemas de votación electrónica (Rodríguez Pérez, 2022) Y sobre todo, como hemos visto, resulta más difícil explicar al público de una manera sencilla los mecanismos técnicos que garantizan dicho secreto. Y en materia de secreto de voto no servirá la experiencia de uso habitual de tecnologías remotas para gestiones administrativas porque en ellas la identificación del votante siempre es expresa y queda unida al trámite. El secreto nunca es el objetivo; más bien al contrario. La clave será -de nuevo- la confianza en las autoridades electorales.

En el caso del voto por internet, los estándares internacionales y constitucionales exigen que la implementación del voto por internet (un voto que busca facilitar la participación) no menoscabe las características esenciales del sufragio. Si bien el voto por internet es una medida idónea y, dada la ineficacia de los canales convencionales, necesaria para fomentar la participación de los residentes ausentes, su principal desafío es equilibrar la comodidad y la accesibilidad con la preservación de la transparencia y la libertad/secreto del voto, que son más difíciles de garantizar en un entorno no presencial.

El voto por internet es como una caja fuerte digital. Debe ser muy fácil de usar para el votante, asegurando que solo él pueda poner su voto dentro (libertad/personalidad) y que el voto, una vez dentro, sea indescifrable y anónimo (secreto). Sin embargo, a diferencia de una caja fuerte física (que puede ser observada por todos para asegurar que nadie la manipule), la "caja fuerte digital" es

opaca para el público, lo que obliga a depender de expertos (verificación) y tecnologías de alta seguridad y fiabilidad para mantener la confianza pública en el resultado (universalidad e igualdad).

8. Recomendaciones

La implementación de un sistema de voto por internet requiere un enfoque riguroso que equilibre la promoción de la participación (el fin legítimo) con el cumplimiento de las características irrenunciables del sufragio (los estándares internacionales y constitucionales).

De ahí que a la hora de establecer recomendaciones que España debería considerar al poner en marcha un sistema de voto por internet, nos basemos tanto en el marco constitucional como en la experiencia internacional:

I. Marco Normativo y Consenso Político

1. Establecer una Previsión Legal Expresa

La introducción de esta modalidad de voto debe realizarse mediante una previsión legal expresa. No es conveniente forzar la literalidad de los preceptos existentes o introducir modificaciones sustanciales por vía reglamentaria, ya que la ley es lo que garantiza el apoyo político necesario.

2. Circunscribir su Uso a Carácter Excepcional y Alternativo

El voto por internet debe ser considerado como una medida excepcional, que funcione como una alternativa a las vías convencionales que deben seguir manteniéndose y mejorándose. Esta modalidad se justifica especialmente para electores que tienen dificultades para ejercer su derecho, como los residentes ausentes (CERA/ERTA), ya que el sistema tradicional es a menudo ineficaz para ellos.

3. Asegurar un Amplio Consenso Público

Es fundamental planificar un amplio debate público para asegurar un grado muy elevado de consenso político y para afianzar la confianza pública en el sistema electoral en su conjunto.

II. Requerimientos Técnicos y de Seguridad (Garantías)

La introducción de esta tecnología conlleva la complejidad de controlar el medio, siendo los principales problemas los ataques informáticos (hackers) y la manipulación interna. Por ello, los requisitos de seguridad son primordiales:

4. Desarrollar un Sistema de Verificación Integral (E2E)

El sistema debe incluir mecanismos para asegurar que el voto se emitió correctamente, se registró como se emitió, y se contó como se registró. Esto se desglosa en:

> Verificabilidad Individual: El elector debe poder comprobar que su voto fue contado y que lo fue con el sentido que él le dio.
> Verificabilidad Universal: Cualquier persona debería poder comprobar que el resultado final corresponde al contenido de la urna electrónica.

5. Garantizar la Seguridad y Fiabilidad del Sistema

Se debe establecer un sistema completo de garantías y requerimientos técnicos para cumplir con los estándares internacionales:

> Control del *Software* y Servidores: Establecer el control sobre los programas que posibilitan la votación, así como la ubicación y control sobre el servidor.
> Seguridad Telemática: Garantizar la seguridad de internet en los países donde se emitiría el voto.
> Planes de Contingencia: Prever planes de emergencia y formas de subsanación en caso de fallos del sistema que pudieran afectar el resultado de la votación.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
red.es
Plan de Recuperación, Transformación y Resiliencia

Garantía de Personalidad: Establecer medios técnicos para garantizar la personalidad del votante (que la persona que vota es quien dice ser).

6. Asegurar el Secreto y la Libertad del Voto

Para cumplir con los principios de Libertad y Secreto del sufragio (Art. 68.1 CE), el sistema debe:

Desconexión Elector-Voto: Preservar el anonimato y el secreto del voto, logrando la desconexión entre el elector identificado y el sentido del voto.

Resistencia a la Coerción: Considerar la posibilidad de que el elector no esté en un entorno vigilado y seguro. El sistema debería ofrecer la posibilidad de re-votar (como en Estonia), lo cual actúa como una defensa contra la coacción al permitir al elector cambiar su voto si se sintió presionado.

III. Proceso de Implementación y Fiscalización

7. Implementación Gradual y Ensayos Detallados

La experiencia internacional demuestra que los países exitosos (como Estonia) han implantado el sistema de manera paulatina y tras múltiples ensayos. El país debe planificar detalladamente el proceso, estableciendo fases y los ensayos precisos para asegurar su correcto funcionamiento.

8. Implementar una Fiscalización Técnica Rigurosa

El sistema debe estar sometido a formas rigurosas de control. Es esencial contar con una fiscalización técnica realizada por agentes diferentes a quienes prestan el servicio. También debe articularse la intervención de los representantes de las candidaturas que concurren a las elecciones y establecer formas de control en favor de las juntas electorales.

9. Establecer Criterios de Anulación Detallados

Aunque la decisión de anular una votación puede recaer en las autoridades legales (abogados) que prefieren la discreción, se recomienda detallar y consolidar en la ley las condiciones para la invalidación (anulación) de los resultados del voto por internet.

IV. Mitigación de Riesgos y Desigualdades

10. Abordar la Brecha Digital y la Universalidad

La universalidad implica que el sufragio debe ser potencialmente ejercido por todos los electores. Dado que el voto por internet requiere conocimientos mínimos de nuevas tecnologías y acceso a internet, se deben mitigar las desigualdades materiales que esto crea:

> Mejora de Alternativas: Conviene mejorar los procedimientos alternativos que se ofrecen, como el voto postal o consular, para no crear desigualdades entre los residentes ausentes "duchos" en la red y quienes no lo son.
> Formación y Conocimiento: Realizar campañas destinadas a garantizar un conocimiento generalizado del sistema y la formación del votante.

11. Gestionar la Falta de Transparencia

El voto por internet implica una ausencia de publicidad y transparencia en comparación con el voto convencional, ya que la verificación pasa a ser monopolizada por expertos informáticos. El país debe sopesar que este inconveniente, aunque se supera por la ventaja de facilitar un derecho fundamental, podría ser objeto de críticas por infringir la universalidad del sufragio (entendida como el control potencial del procedimiento por parte del cuerpo electoral).

12. Utilización Auxiliar de Internet a Corto Plazo

Incluso antes de la implementación completa del voto por internet, la tecnología puede utilizarse como instrumento auxiliar. Por ejemplo, podría utilizarse para que el

elector descargue telemáticamente las papeletas de votación (previa reforma legal), lo que ahorraría tiempo en la fase de remisión de documentación electoral.

9. Bibliografía

Abel, L. (2018). Trust in ICT for the public sector: E-voting in Brazil's 2014 election.

Agrawal, P., Sharma, S., & Subhashis Banerjee. (2021). Unsuitability of internet voting, and *blockchain* vs public bulletin board for integrity of elections and electoral rolls. Disponible en: https://www.cse.iitd.ac.in/~suban/reports/bcvbb.pdf

Avgerou, C. (2013). Explaining Trust in IT-Mediated Elections: A Case Study of E-Voting in Brazil. J. Assoc. Inf. Syst., 14, 2. https://doi.org/10.17705/1jais.00340

Benaloh, J. y Tuinstra, D. (1994). Receipt-free secret-ballot elections. *STOC*, 1994.

Blaze, M. (2017). US House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs. Hearing on Cybersecurity of Voting Machines. Noviembre, 2017.

Boucher, P. (2017). How *blockchain* technology could change our lives. *EPRS,* 2017

Castells, M. (1997). La era de la información: economía, sociedad y cultura. Vol. 1 Alianza Editorial.

Dandoy, R. (2021). An Analysis of Electronic Voting in Belgium. En D. Caluwaerts & M. Reuchamps, Belgian Exceptionalism (1.a ed., pp. 44-58). Routledge. https://doi.org/10.4324/9781003104643-5

Daoudi, Bouchra. (2021). Contester les algorithmes sur le terrain électoral : le cas des machines à voter en France. Éthique Publique, vol. 23, n° 2. https://doi.org/10.4000/ethiquepublique.6573

Das, S. (3 September 2018). In a First, Japanese City Deploys Online *blockchain* Voting System. *CCN*. Disponible en: https://www.ccn.com/in-a-first-japanese-city-deploys-online-*blockchain*-voting-system/

Debant, A., & Hirschi, L. (2023). Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. 32nd USENIX Security Symposium (USENIX Security 23), 6737–6752. https://www.usenix.org/conference/usenixsecurity23/presentation/debant

Duenas-Cid, D. (2024). Trust and Distrust in electoral technologies: What can we learn from the failure of electronic voting in the Netherlands (2006/07). Proceedings of the 25th annual international conference on digital government research, 669-677. https://doi.org/10.1145/3657054.3657262

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly, 39(4), 101718. https://doi.org/10.1016/j.giq.2022.101718

Enguehard, C. (2007). Le vote électronique en France: opaque & invérifiable. Terminal. Technologie de l'information, culture & société, (99-100), 199-214.

Enguehard, C., & Noûs, C. (2020). Some Things you may Want to Know about Electronic Voting in France. Hal.science. https://cnrs.hal.science/hal-02951467

Fujiwara, T., & Fujiwara, T. (2015). Voting Technology, Political Responsiveness, and Infant Health: Evidence From Brazil. Econometrica, 83, 423-464. https://doi.org/10.3982/ECTA11520

Giannopoulou, A. & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review, 10* (2). https://doi.org/10.14763/2021.2.1550

Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of E-voting: The past, present and future. Annals of Telecommunications, 71(7), 279-286. https://doi.org/10.1007/s12243-016-0525-8

Guglielmi, G. (2017). El voto electrónico atrapado por el Derecho. El caso francés [Review of El voto electrónico atrapado por el Derecho. El caso francés]. In G. Guglielmi (Ed.), El voto electrónico (pp. 181–198). Centro de Estudios Políticos y Constitucionales.

Jacobs, B., & Pieters, W. (2009). Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment. En A. Aldini, G. Barthe, & R. Gorrieri (Eds.), Foundations of Security Analysis and Design V (Vol. 5705, pp. 121-144). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03829-7_4

Juels, A, Catalano, D. Jakobson, M. Coercion-resistant electronic elections. WPES, 2005.

Kshetri, N. & Voas, Jeffrey. (2018). *Blockchain*-Enabled E-Voting. *IEEE Software*. 35. 95-99. 10.1109/MS.2018.2801546.

Loeber, L. (2008). E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years. 21-30.

Magnuson, W. (2020). *Blockchain Democracy: Technology, Law and the Rule of the Crowd.* Cambridge University Press.

Nicolau, J. (2019). The Electronic Voting Machine and the Improvement of the Elections in Brazil.

Park, S., Specter, M., Narula, N., Rivest, Ronald L., MIT, (2021). Going from bad to worse: from Internet voting to *blockchain* voting, *Journal of Cybersecurity, 7* (1), 2021. https://doi.org/10.1093/cybsec/tyaa025

Parsovs, A. (2020). Solving the Estonian ID card crisis: The legal issues. ISCRAM 2020 conference proceedings-17th international conference on information systems for crisis response and management, 459-471.

Renaud-Garabedian, É. (2024, 18 de julio). *Dysfonctionnements du vote électronique durant les élections législatives 2024* (Question écrite n° 12475). Journal Officiel du Sénat. https://www.senat.fr/questions/base/2024/qSEQ240712475.html

Rodríguez Pérez, A. (2022). Secret texts and cipherballots: Secret suffrage and remote electronic voting [Ph.D. Thesis, Universitat Rovira i Virgili]. En TDX (Tesis Doctorals en Xarxa). https://www.tdx.cat/handle/10803/675606

Rubio, R., & Malikbayeva, S. (2023). *Blockchain*: Gobierno y democracia. Casos de uso de *blockchain* en la administración (con atención especial a las votaciones). En Criptoderecho. La regulación de *Blockchain* (2a). La Ley.

Rubio, R. Vela Navarro-Rubio, R. (2017) Parlamento Abierto: El Parlamento en el siglo XXI. Editorial UOC.

Schäffner, M. (n.d.). *Blockchain*-enabled Self-Sovereign Identity. *Zigurat*. https://www.e-zigurat.com/innovation-school/blog/self-sovereign-identity

Schneider, R., & Senters, K. (2018). Winners and Losers of the Ballot: Electronic vs. Traditional Paper Voting Systems in Brazil. Latin American Politics and Society, 60, 41-60. https://doi.org/10.1017/lap.2018.5

Spoormans, H. (2019). La experiencia «Orange». La laboriosa introducción del voto electrónico en Holanda. Teoría y Realidad Constitucional, 44, 437. https://doi.org/10.5944/trc.44.2019.26013

Torres García, J. J. 2022. Introducción a la criptografía del voto electrónico, en Crítica interdisciplinar de los sistemas de votación electrónica: revisando la democracia digital. EOLAS. pp.. ISBN 978-84-18718-64-9.

Trippi, J. (2004). *Revolution will not be televised*. New York. Regan Books. 2004.

Rodríguez Pérez, A. (2022). Secret texts and cipherballots: Secret suffrage and remote electronic voting [Ph.D. Thesis, Universitat Rovira i Virgili]. En TDX (Tesis Doctorals en Xarxa). https://www.tdx.cat/handle/10803/675606

Vinnakota, R. (22 enero 2021). Which Countries Are Casting Votes Using *blockchain*? Hackernoon. Disponible en: https://hackernoon.com/which-countries-are-casting-voting-using-*blockchain*-s33j34ab

Zambrano, R. (2017). Unpacking the disruptive potential of *blockchain* technology for human development. *International Development Research Center.* Disponible en: https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

Zhang, S., Wang, L. & Xiong, H. (2020). Chaintegrity: *blockchain*-enabled large-scale e-voting system with robustness and universal verifiability. *Int. J. Inf. Secur.* 19, 323–341 (2020). https://doi.org/10.1007/s10207-019-00465-8

Sentencias:

BVerfG, Judgment of the Second Senate of 3 March 2009 - 2 BvC 3/07 -, paras. 1-166

Tribunal Supremo de Estonia 5-19-18, de 27 de marzo

Tribunal Constitucional Alemán, BVerfGE 21, 200 [205]

Informes:

Análisis jurídico, técnico, organizativo y presupuestal de las alternativas sobre el voto de los mexicanos residentes en el extranjero que presenta Comité Técnico de especialistas creado por acuerdo CG753/2012 (https://votoextranjero.mx/documents/52001/54190/An%C3%A1lisis+CTE-VMRE_Resumen+ejecutivo_VF_a.pdf/5aa46320-10bc-4ed0-a527-0bebaf323dc5)

Comisión de Venecia (2002). Code of Good Practice in Electoral Matters.

Comité de DDHH de Naciones Unidas. Observación General 25 (1996) sobre "El derecho a participar en los asuntos públicos, el derecho al voto y el derecho de acceso a cargos públicos en condiciones de igualdad".

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

Plan de Recuperación, Transformación y Resiliencia

European Commission. Directorate General for Justice and Consumers. (2023). Compendium of e-voting and other ICT practices: Non paper from the Commission services. Publications Office. https://data.europa.eu/doi/10.2838/464803

Electoral Central, J. (2019). Informe de la Junta Electoral Central de 16 de noviembre de 2016, sobre la regulación del voto de los electores españoles que residen o se hallan en el extranjero. Revista De Las Cortes Generales, (107), 425-468. https://doi.org/10.33426/rcg/2019/107/1452

Gencat (13 septiembre 2019). Catalan government plans to introduce self-sovereign identity platform. Disponible en: https://catalangovernment.eu/catalangovernment/news/377238/catalan-government-plans-to-introduce-self-sovereign-identity-platform Más información en: https://politiquesdigitals.gencat.cat/ca/ciutadania/identicat

Guidelines on the use of information and communication technology (ICT) in electoral processes en 2023 (CM(2022)10-final)

IDEA. (2023). Use of E-Voting Around the World [Dataset]. https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world

Instituto Nacional Electoral. (2024, 29 de agosto). *Informe final de actividades sobre el PIT-VMRE (Plan Integral de Trabajo del Voto de las Mexicanas y los Mexicanos Residentes en el Extranjero para los Procesos Electorales Federal y Locales 2023-2024)*. https://repositoriodocumental.ine.mx/xmlui/handle/123456789/176656

Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting