REVISTA DERECHO ELECTORAL
PRIMER SEMESTRE 2021 NÚMERO 31
ISSN: 1659-2069

El análisis FODA del voto electrónico y perspectivas de futuro

J. Angelo Berbotto*

https://doi.org/10.35242/RDE_2020_31_10

Nota del Consejo Editorial

Recepción: 6 de octubre de 2020.

Revisión, corrección y aprobación: 18 de diciembre de 2020.

Resumen: Las nuevas tecnologías aplicadas a los procesos electorales ya están en uso desde hace unos treinta años. Sin embargo, no se constata su uso masivo. El análisis FODA de dichas tecnologías es una herramienta para revelar las razones de esto y valorar las perspectivas de futuro del voto electrónico.

Palabras clave: Voto electrónico / Automatización de los procesos electorales / Máquinas para votar / Papeleta electrónica / Urna electrónica / Tecnologías de información / Análisis FODA.

Abstract: New technologies applied to electoral processes have been around for over thirty years. However, they have not been adopted in large numbers. The SWOT analysis of e-voting provides a tool to ascertain why that is the case and to assess its future.

Key Words: E-vote / Automated electoral processes / Voting machines / E-ballot / Electronic ballot box / Information technologies / SWOT analysis.

* Uruguayo-australiano, abogado, correo angelo.berbotto@gmail.com. Licenciado en Derecho por la Universidad Tecnológica de Sydney (2004), máster en Redacción de Legislación, Regulación y Políticas por la Universidad de Londres (2019), egresado de la maestría de Derecho Parlamentario, Elecciones y Estudios Legislativos de la Universidad Complutense de Madrid (2020). Actualmente redactor legislativo en la Office of the Queensland Parliamentary Counsel, Australia.

ISSN: 1659-2069

1. INTRODUCCIÓN

A fines del siglo XX se empieza a experimentar tímidamente con las nuevas tecnologías en el ámbito electoral. Ya entrado el nuevo siglo, el Consejo de Europa, reconociendo el aumento de las experiencias con las nuevas tecnologías, estableció una comisión *ad hoc* de expertos jurídicos sobre las normas legales, operacionales y técnicas del voto electrónico que dieron como resultado la Recomendación Rec(2017)5, aprobada el 14 de junio de 2017, sobre las normas relacionadas con el voto electrónico.

La Rec(2017)5 invitaba a los Gobiernos de los Estados miembros a respetar, en la legislación interna, así como en la utilización del voto electrónico, todos los principios de las elecciones democráticas. También los instaba a adoptar el Anexo de la Rec(2017)5 y expresaba que se debería tomar en cuenta, para su implementación, la interconexión entre las normas citadas y las directrices.

Excepto algunos casos aislados, no ha habido una adopción importante del voto electrónico. Al contrario, en muchas jurisdicciones pioneras en las experiencias con el voto electrónico se ha abandonado. Este artículo utiliza la metodología de la matriz FODA para revelar las fortalezas, las oportunidades, las debilidades y las amenazas del voto electrónico, así como para identificar qué modalidades han sido bien recibidas por los organismos de gestión electoral nacionales y la razón para ello.

2. ¿QUÉ ES EL VOTO ELECTRÓNICO?

El glosario del Anexo II de la Rec(2017)5 define voto electrónico como la utilización de medios electrónicos para votar y/o contar los votos. Esta definición abre un abanico de situaciones: desde los sistemas no conectados a una red cuyo software atiende a las necesidades de almacenamiento y recuento del voto, pasando por aquellos conectados a internet en cabinas electorales, así como los sistemas de voto electrónico remoto (a través de mensaje de texto desde un teléfono móvil, por internet o email) con softwares altamente sofisticados.

Las experiencias con el voto electrónico comienzan a fines del siglo XX. En 1989, en Bélgica estudian adoptar el voto electrónico (Fernández, 2001), y en 1991 se despliega una experiencia piloto en el cantón de Verlaine, seguida en 1994 por el cantón de Luik. En Francia se utilizó el voto electrónico en Estrasburgo para las elecciones europeas de junio de 1994

ISSN: 1659-2069

y en 1995 en Issy-Les-Moulinaux para las elecciones presidenciales. En 1995, el Gobierno de Brasil comenzó a explorar la posibilidad de implementar el voto electrónico que luego llevó a cabo (Lheureux de Freitas et al., 2017).

Entre 1992 y 1995 se hicieron igualmente diferentes pruebas en Noruega y en Dinamarca. En 2001, Estonia anunció su intención de introducir el voto electrónico, el cual se utilizó por primera vez en las elecciones municipales de 2005 (D'Onofrio, 2014). Como se puede apreciar, los países que han experimentado con el voto electrónico son variados.

Fernández (2001) señala que en España las experiencias han sido exclusivamente a nivel de las Comunidades Autónomas: en 1995, en las elecciones autonómicas al Parlamento de Cataluña se utilizó el voto electrónico en dos colegios electorales; en 1997, en Galicia dos colegios electorales de Santiago de Compostela utilizaron el voto electrónico (cada mesa empleó un sistema y tecnología diferente); y también en 1997, en las elecciones de las Cortes Valencianas se utilizó el voto electrónico en el municipio de Villena paralelamente al procedimiento ordinario de votación por papeleta.

En 1998, el Parlamento Vasco modificó la Ley 5/1990, del 15 de junio, de Elecciones al Parlamento Vasco a fin de poder utilizar el voto electrónico en las elecciones autonómicas. Sin embargo, en las elecciones siguientes, del 13 de mayo de 2001, no se usó el voto electrónico, aunque el procedimiento estuviera dispuesto en una ley vigente, lo cual fue criticado como falta de coherencia (Fernández, 2001).

Estos antecedentes históricos son prueba del interés por la experimentación con las nuevas tecnologías aplicadas a los procesos electorales. A continuación, analizamos las tres modalidades del voto electrónico.

3. LAS MODALIDADES DEL VOTO ELECTRÓNICO

Podemos distinguir dos grupos de tecnologías del voto electrónico según estén o no conectadas a una red. En el **voto electrónico no conectado a una red** ubicamos las tarjetas perforadas y otras que utilizan la tecnología de lectura óptico-electrónica para el escrutinio (Fernández, 2001). También están las terminales de pantalla sensible al tacto en las que el votante puede elegir el voto, el cual queda registrado en el

ISSN: 1659-2069

ordenador; este necesita un proceso manual para luego recuperar, en un artefacto de memoria portátil, todos los votos realizados y trasladarlos al sitio donde se hará el recuento (Mercurio, 2002).

Un sistema de este tipo se utiliza en Brasil donde se valen de unas terminales portátiles, diseñadas para su utilización en las partes del país sin corriente eléctrica (Lheureux de Freitas et al., 2017). La interface del sistema no es muy diferente a la de los cajeros automáticos: al votar, la máquina imprime un recibo que el votante puede verificar y anular y comenzar de nuevo en caso de error (Mercurio, 2002).

La modalidad de voto electrónico conectado a una red admite dos subcategorías: el voto electrónico en un entorno controlado y el voto remoto (Loncke et al., 2004,).

En el **voto electrónico en un entorno controlado**, la votación se realiza en las mesas electorales, donde en vez de la papeleta tradicional se utiliza un ordenador conectado a un servidor central (Mercurio, 2002). Las terminales están sujetas a la inspección y supervisión de la mesa, lo que permite controlar que el elector vote en privado, sin influencias de terceros, tal como sucede cuando vota con la papeleta tradicional (Loncke et al., 2004).

En los **sistemas de voto remoto** se utiliza el ordenador personal (o el teléfono móvil) para votar; pero al no estar en un entorno controlado, no es posible asegurar la privacidad del elector o la ausencia de intimidación o soborno (Schwartz y Grice, 2013). Las condiciones que existen en las elecciones tradicionales no se pueden replicar cuando el voto se hace de manera remota (Loncke et al., 2004).

4. LA MATRIZ FODA

Pérez (2011, p. 2) define la matriz FODA (o DAFO) como una herramienta de múltiple aplicación, útil para analizar diferentes aspectos de carácter estratégico, que informa la toma de decisiones y que permite enterarse de las condiciones reales en que se encuentra un producto u organización para asumir el riesgo y aprovechar las oportunidades que le brinda el entorno. En esta sección sometemos las tres modalidades del voto electrónico al análisis FODA.

ISSN: 1659-2069

4.1 LAS FORTALEZAS

Las fortalezas son las capacidades particulares con que cuenta cada modalidad del voto electrónico, y que le permiten tener una posición privilegiada (Pérez, 2011).

En relación con el voto electrónico no conectado a la red, Bernhard (2017) señala que una de sus fortalezas es que permite verificar el recuento de los votos manualmente para confirmar que la tecnología ha funcionado como previsto. Un ejemplo es el método Mercuri que, sin entregar un comprobante al elector, le permite ver impreso su voto, el cual se deposita también en papel y de manera automática en una urna por si es necesario el recuento manual (Presno, 2016). Lo anterior está en sintonía con la norma 17 de la Rec(2017)5 que dispone que el voto electrónico debe producir pruebas tangibles de que cada voto auténtico se ha incluido correctamente en los resultados electorales respectivos y que los elementos de prueba han de verificarse por medios independientes del sistema de voto electrónico.

Otra fortaleza es que mantiene el requisito de asistir a las urnas el día de las elecciones, lo cual Svensson y Leenes (2003) identifican como de importancia simbólica al mantenerse este ritual de la democracia representativa en la que todos los ciudadanos depositan sus votos en un plano de igualdad.

Al no estar conectado a una red, resulta más sencillo velar por la integridad y la seguridad del voto. El tipo de software necesario para desarrollar esta modalidad de voto debe atender a la integridad del almacenamiento de los datos y garantizar la lectura de las papeletas. Pero su funcionamiento autónomo y no conectado a una red disminuye el riesgo de manipulación externa y, por consiguiente, los ataques externos no son necesariamente los objetivos principales del software, sino la lectura eficaz y el almacenamiento fiables.

En Gujarat, India, el sistema requiere que tres titulares de tarjetas inteligentes (que pueden ser la presidencia de la mesa) las utilicen para poder comenzar y finalizar el escrutinio (Schwarts et al., 2013). Por las razones enunciadas, este sistema es también más resistente a la interferencia exterior como los ataques de hackers (Mercurio, 2002).

En los años 90 en Brasil se utilizaba un sistema de voto electrónico no conectado a la red, consistente en terminales portátiles autónomas que

ISSN: 1659-2069

funcionaban a batería (diseñadas para trasladarlas a lugares remotos), con una interface numérica (Lheureux de Freitas et al., 2017). En 2007, Jamaica implementó el voto electrónico no conectado a la red con el fin de impedir la votación múltiple y el uso de papeletas falsas. Los electores que figuran en el padrón se identifican en las mesas mediante huellas dactilares y a continuación el sistema emite papeletas autenticadas para votar (Lheureux de Freitas et al., 2017).

Una fortaleza del **voto electrónico conectado a la red en un entorno controlado** es que se preserva el ritual de ir a las urnas (Svensson y Leenes, 2003). Otra fortaleza radica en la capacidad de imprimir registros y permitir un posterior recuento manual (Schwartz y Grice, 2013). Asimismo, permiten un recuento inmediato y el anuncio de los resultados al cierre de las mesas (Mercurio, 2004).

Las fortalezas del **voto electrónico remoto** son la comodidad de poder votar desde cualquier sitio (Loncke et al., 2004), lo que favorece a los votantes rurales, a quienes tienen responsabilidades laborales o de cuidado del hogar y a los enfermos y discapacitados imposibilitados de trasladarse. En estos casos el voto remoto favorece la igualdad de acceso y contribuye a una mayor participación en las elecciones (Schwartz y Grice, 2013). Este hace posible cambiar el voto antes de que cierren los comicios, así funciona en Estonia, y se cuenta el último voto realizado (D'Onofrio, 2014). Esta opción está en armonía con la norma 12 de la Rec(2017)5 que dispone que el voto electrónico debe permitir al elector la posibilidad de confirmar su voto; y la norma 25 sobre la garantía del secreto de las selecciones precedentemente registradas y luego anuladas por el elector antes de la expresión definitiva de su voto. También es una fortaleza la capacidad de hacer un recuento inmediato y anunciar los resultados de las elecciones al cierre de las mesas (Mercurio, 2004). Estonia continúa usando el voto electrónico remoto. Para 2016 ya había realizado tres elecciones con voto remoto, con la verificación de una ausencia de ataques a gran escala o manipulaciones (Vinkel et al., 2016).

4.2 LAS OPORTUNIDADES

Son oportunidades aquellos factores que resultan positivos, favorables, explotables, que se deben descubrir en el entorno en el que actúa la organización / producto, y que permiten obtener ventajas competitivas (Pérez, 2011).

ISSN: 1659-2069

Una oportunidad del **voto electrónico no conectado a la red** es que el gasto inicial elevado de adquirir las terminales se puede amortizar en elecciones futuras al ser el equipamiento reutilizable (Gálvez et al., 2011) siempre y cuando no resulte obsoleto.

Con relación a las oportunidades **del voto electrónico conectado a la red en un entorno controlado,** el gasto inicial se puede amortizar, pero persisten gastos considerables de soporte técnico para mantener la integridad de la red, verificar la no intervención de las terminales y reparar las fallas en el sistema. Otra oportunidad es su capacidad para evitar los recuentos exigidos por el candidato perdedor, ya que el voto electrónico recoge resultados exactos, por lo que elimina el margen de error humano (Mercurio, 2004).

Las oportunidades del **voto electrónico remoto** radican en un potencial aumento del número de electores, al facilitar el acceso al proceso de votación y dispensar con la visita a la mesa (Hermanns, 2008). El voto remoto es de interés particular para grupos con dificultad de movilidad como los ancianos, los cuidadores y los discapacitados, ya que este método es más accesible (Loncke et al., 2004). A propósito, la norma 2 de la Rec(2017)5 dispone que el sistema de voto electrónico debe ser concebido de manera que permita votar a los electores con discapacidad y a las personas que tengan necesidades especiales, de forma autónoma. Otra oportunidad reside en la capacidad para evitar los recuentos, pues elimina el margen de error humano lo cual reduce los motivos para exigir un recuento aun cuando la diferencia de votos sea escasa (Mercurio, 2004).

4.3 LAS DEBILIDADES

Las debilidades son aquellos factores que provocan una posición desfavorable frente a la competencia, recursos que faltan, habilidades que no se poseen, actividades que no se desarrollan positivamente y otros factores similares (Pérez, 2011)

Una debilidad **del voto electrónico no conectado a la red** es que a los elevados gastos de adquisición hay que sumarles los de su almacenamiento en un recinto lo suficientemente amplio y seguro para evitar que se interfiera con este. Además, hay que tener en cuenta su potencialmente limitada vida útil, ya que el riesgo de que la tecnología resulte obsoleta al cabo de pocos años es considerable. Otra debilidad es

ISSN: 1659-2069

la necesidad de formar al organismo de gestión electoral (Gálvez et al., 2011), así como a los integrantes de las mesas en el funcionamiento de las máquinas y la manera de hacer frente a imprevistos. Otra debilidad es el riesgo de que la tecnología falle como ocurrió en 2004 en EEUU, cuando los errores de sistema resultaron en la pérdida o en la no contabilización de votos en Florida y Carolina del Norte (Coney, 2005); por ello, es esencial poner a prueba la tecnología de forma rigurosa antes de desplegarla a grande escala en las elecciones. Igualmente ocurrió en Finlandia en las elecciones municipales de 2008. La municipalidad de Grankulla y otras dos aledañas utilizaron el voto electrónico como parte de un proyecto piloto. La prueba fue un fracaso, las elecciones en las tres municipalidades tuvieron que anularse y volverse a repetir a causa de las pruebas insuficientes que se realizaron del programa utilizado (Wrede, 2016).

Con respecto al **voto electrónico conectado a la red en un entorno controlado**, *una debilidad* es el elevado costo para adquirir el sistema y para guardarlo en el período entre elecciones (Schwartz y Grice, 2013). Otra debilidad es el arduo trabajo de puesta a prueba del sistema, ya que cada terminal puede ser objeto de manipulación o mal funcionamiento. Una terminal averiada podría afectar los resultados, puesto que puede almacenar cientos de votos, con lo que se afectan potencialmente los resultados de una elección mediante la instalación de software dañino en un pequeño número de máquinas (Schwartz y Grice, 2013). Los procedimientos de seguridad para evitar la manipulación e interferencias externas no son infalibles, las experiencias recientes lo demuestran. En los Países Bajos, se constató que era posible instalar software malicioso en el sistema específico que el Gobierno estaba utilizando y que era posible averiguar qué habían votado los electores al observar las señales electromagnéticas que emitían los monitores análogos utilizados en ese momento (Schwartz y Grice, 2013).

Entre las debilidades del **voto electrónico remoto** está la gran inversión que representa diseñar el sistema, máxime cuando no logra los resultados esperados en materia de electores que lo utilicen. Schwartz y Grice (2013) citan los ejemplos de Australia y Canadá al respecto. En 2004, la Comisión Electoral Australiana utilizó el voto por internet para el personal militar en Australia a un costo de aproximadamente 320 euros por elector en comparación con 6 euros al utilizar el método tradicional, o sea 50 veces más costoso. En Canadá, la tecnología para un proyecto piloto con el voto remoto en las elecciones federales parciales en Winnipeg en 2010 costó

ISSN: 1659-2069

aproximadamente 26 600 euros y solamente cinco electores lo utilizaron, prueba de la desconfianza que todavía inspira el uso de esta tecnología en las elecciones, como lo señalan las siguientes debilidades identificadas.

Se percibe como debilidad el traslado del acto público de los comicios, que reúne a la ciudadanía, a la esfera privada con la consiguiente pérdida del carácter visible, público y simbólico del voto (Svensson y Leenes, 2003). Además, al votar en privado es difícil garantizar que sea realmente el elector quien emite el voto y no otra persona en su lugar. La norma 7 de la Rec(2017)5 establece que la identificación exclusiva de los electores debe ser asegurada de manera que permita distinguirlos sin que quepa duda alguna; y la norma 8 de la Rec(2017)5 dispone que el sistema de voto electrónico no autorizará el acceso de un usuario a menos que sean previamente identificados como personas habilitadas para votar.

Otra debilidad es que el voto remoto no da garantías contra la venta de votos. En Estonia, donde los ciudadanos votan por internet utilizando su documento de identidad, es posible que una persona use el documento y el PIN de otra. Lo mismo puede ocurrir en sistemas de voto mediante telefonía móvil. Si una persona tiene acceso al móvil de otra, podrá fácilmente depositar el voto en su lugar (Hamed y Sedky, 2016).

En torno a la falta de supervisión, el voto remoto no hace posible cerciorarse de que el elector ejerce su derecho al voto en un ambiente de plena libertad, sin coacción de ningún tipo (Gálvez, 2009). La norma 10 de la Rec(2017)5 dispone que la intención del elector no será afectada por el sistema de voto y estará amparada de toda influencia indebida. Svensson y Leenes (2003) consideran como una debilidad la falta de supervisión capaz de atentar contra el secreto del voto, el cual se considera un elemento crucial en las elecciones de los Estados modernos y ha sido un principio adoptado en varias convenciones y declaraciones como la Declaración Universal de Derechos Humanos (artículo 21, numeral 3), el Pacto Internacional de Derechos Civiles y Políticos (artículo 25) y la Convención Europea de Derechos Humanos (Protocolo 1, artículo 3).

Las normas 19 a 26 de la Rec(2017)5 reúnen una serie de principios, lo que demuestra la importancia del secreto del voto. Resaltamos la norma 19 que dispone que el voto electrónico debe ser organizado de manera que garantice que se respete, en todas las etapas del proceso, el secreto del sufragio. Asimismo, la norma 20 establece que el sistema de voto electrónico no debe gestionar ni almacenar, más del tiempo que sea

ISSN: 1659-2069

necesario, los datos personales requeridos para realizar las elecciones electrónicas. La norma 21 dispone que el sistema de voto electrónico y toda parte autorizada deben proteger los datos de autenticación a fin de impedir que las partes no autorizadas distorsionen, intercepten, modifiquen o de algún otro modo lleguen al conocimiento de dichos datos.

En 2016, Unt et al. (2016) demostraron cómo el derecho al voto secreto en Estonia podía ser violado. Utilizaron registros informáticos para identificar sesiones de voto electrónico que provenían de la misma dirección IP y ordenadores que usaban el mismo sistema operativo y en las que las sesiones para depositar el voto se espaciaban más de 10 minutos entre el fin de una sesión y el comienzo de otra. De esta manera, Unt et al. fueron capaces de identificar las dinámicas de la votación, por ejemplo, cuándo dos votos que se depositaban en sucesión correspondían a matrimonios y cuándo los votos eran los de padres e hijos adultos que votaban desde la misma dirección IP.

Otra debilidad es que el voto remoto necesita una sociedad madura en el ámbito de la digitalización, preparada para los desafíos que el uso del voto remoto representará (ataques de ciberpiratas, averías, fallas, etc.). En Estonia, la votación remota es parte de un proceso de digitalización a grande escala donde, resaltan Schwartz y Grice (2013), la identificación y autenticación de los electores se realiza mediante la tarjeta de identificación electrónica nacional que a su vez se utiliza para diversas tareas desde recargar el billete de autobús hasta acceder a servicios estatales. Para votar, los electores colocan la tarjeta dentro de un lector que está conectado al ordenador y digitan una clave. La tarjeta contiene un código que encripta de modo seguro su identificación y, en caso de pérdida, es posible obtener otra en un banco o ventanilla de un ente estatal. El riesgo de que alguien no autorizado participe en las elecciones es reducido, ya que, a fin de obtener la tarjeta y la clave, los ciudadanos deben primero aportar pruebas de su identidad.

Algunos estados se valen de otros métodos a fin de minimizar el riesgo de fraude con el voto remoto. En India, para poder usar el voto remoto, es necesario presentarse para registrar los datos biométricos (huellas dactilares) y así recibir la tarjeta electoral y un PIN (Schwartz y Grice, 2013). Aun siendo muy prudente, no se pueden descartar las fallas y el mal funcionamiento del sistema, ya que la tecnología no da garantías totales, por ejemplo el proyecto SERVE (*Secure Electronic Registration and Voting Experiment* del Gobierno de los EE. UU. diseñado para permitir

ISSN: 1659-2069

el voto de los ciudadanos que vivan fuera del país y para el personal militar destinado en el extranjero, fue abandonado ante los numerosos fallos de seguridad que lo hacían vulnerable a los ataques informáticos y por la insuficiente garantía de la confidencialidad del voto (Presno, 2016). Otros casos en los que la implementación del voto remoto no tuvo éxito son los de Washington DC, Inglaterra y los Países Bajos donde el voto remoto o bien se abandonó antes de las elecciones o su uso fue descontinuado luego de haber sido utilizado una vez (Schwartz y Grice, 2013).

4.4 LAS AMENAZAS

Las amenazas son las situaciones que provienen del entorno y que pueden llegar a atentar incluso contra la permanencia de la organización / producto (Pérez, 2011).

Las amenazas contra el **voto electrónico no conectado a la red** no son tan altas como en las otras dos modalidades. Identificamos el ataque exterior de las terminales como una amenaza (Mercurio, 2002), el cual implica proximidad física al no conectarse a una red, por lo que resulta posible imponer medidas para prevenir la interferencia con las máquinas.

La gran amenaza contra **el voto electrónico conectado a la red en un entorno controlado** es la infiltración de piratas informáticos para intervenir el software del sistema. Los piratas buscan la oportunidad de plantar virus mediante descargas desde internet, correo electrónico o al explotar un error en el programa o fallas en la seguridad del ordenador o interface. Los ataques son comunes y es difícil, cuando no imposible, defenderse de ellos (Mercurio, 2002). Una vez que el virus se ha plantado, el pirata informático puede espiar la manera en que votan los electores, impedir a los electores la posibilidad de votar o modificar el voto que han realizado. Además, es posible que el pirata informático logre realizar estas actividades sin haber sido detectado por los electores ni por las medidas de seguridad del sistema de voto remoto, como los dispositivos de criptografía o los programas antivirus. Un virus lanzado para interferir con las elecciones de un país puede causar estragos en el secreto de voto y en la integridad de la elección (Mercurio, 2002).

ISSN: 1659-2069

Igual que en el caso precedente, la mayor amenaza contra el **voto electrónico remoto** es la infiltración de piratas informáticos. El voto remoto se vale de la tecnología criptográfica para mantener el carácter secreto del voto: cuando un elector vota desde su casa, se aplica una avanzada fórmula matemática para encriptar la información a fin de transferirla de manera segura. Para leer el voto, el lector debe poseer la llave criptográfica con las instrucciones para descodificar la información. Los votos se almacenan en un servidor central y la observación de dicho servidor no permitiría que se descifre cómo alguien ha votado hasta el momento en que se encriptó el voto (Schwartz y Grice, 2013). Sin embargo, no es imposible infiltrarse en un sistema y esta es la especialidad de los *hackers*. Este problema se acucia cuando el voto electrónico se utiliza desde fuera del país, ya que el sistema se expone a un número elevado de ciberataques. Un ataque a Estonia ocurrido en 2007, presuntamente de Rusia, causó perturbaciones a los bancos y a la comunicación parlamentaria de Estonia durante casi tres semanas (Schwartz y Grice, 2013). Según los expertos en materia de seguridad, los cuatro países de donde se originaron la mayoría de los ataques informáticos en 2012 fueron China (30,6 %), los EE. UU. (19,2 %), Rusia (13,4 %) e India (9,5 %). Puede que las autoridades electorales tengan que bloquear el acceso desde el extranjero en caso de detectar un ciberataque proveniente de un país extranjero (Schwartz y Grice, 2013).

Hermanns (2008, p. 75) subraya cómo la seguridad del voto remoto con respecto a la verificación y el secreto del voto continúan siendo un desafío, como lo demuestra la experiencia de Noruega, donde en 2009 se desplegó un proyecto piloto que se puso en práctica en las elecciones de 2013. Se utilizó un sistema de voto remoto en el que las papeletas electrónicas se mandaron por canales que se esperaba fueran seguros. En realidad, luego se descubrió que cualquier persona con acceso a ciertos servidores podía comprometer la privacidad de cualquier voto que el elector depositara electrónicamente. La falla tendría que haber sido detectada con la revisión interna del código por el mismo desarrollador. El diseño del programa fue capaz de soportar la catastrófica falla criptográfica sin que ocurriera una fuga de datos privados y la falla al final no atentó contra la integridad de los resultados de la elección; de todas maneras, con el cambio de Gobierno en Noruega se abandonó el proyecto de utilización del voto remoto y se volvió a la tradicional papeleta (Bull et al., 2016).

ISSN: 1659-2069

Otra amenaza del voto remoto es la privación del derecho al voto a causa de la brecha digital. Esta es una inquietud presente en los EE. UU. donde se teme que abrirse al voto electrónico podría quizás aumentar la participación de un grupo (los que tienen acceso a internet) mientras que la participación en las elecciones permanezca invariable en otros grupos (los que no tienen acceso a internet) o sea que la brecha digital resulte en mayor participación entre los electores con mayor nivel de educación y nivel económico a costa de los electores menos educados y más pobres (Mercurio, 2004). Sin duda sería discriminatorio si en las elecciones se permitiera solamente el voto remoto sin hacerlo disponible en lugares públicos como las mesas electorales porque sería una manera irrazonable de eliminar a una parte de la población que no tiene acceso a un ordenador (o teléfono móvil) (Loncke et al., 2004).

5. CONCLUSIONES

La matriz FODA ha puesto en particular evidencia las debilidades y las amenazas del voto electrónico para las modalidades tanto del conectado a la red en un entorno controlado como del voto electrónico remoto. Si bien todas las modalidades presentan fortalezas y oportunidades, las debilidades y amenazas de estas dos modalidades particulares son tales que pueden llegar a poner en peligro la seguridad del resultado electoral, con consecuencias nefastas para las sociedades afectadas.

Con la excepción de Estonia, donde el voto remoto ha sido adoptado y parece funcionar correctamente, otras jurisdicciones han dado marcha atrás en sus experimentos con el voto remoto y el voto conectado a la red en un entorno controlado al reconocer la magnitud de los riesgos existentes. Por ello, es de esperarse que los organismos de gestión electoral nacionales apuesten por tecnologías electorales que ayuden y agilicen el proceso electoral, pero que también minimicen los riesgos. Este es el caso del voto electrónico no conectado a la red, ya que estas tecnologías, por ejemplo, las que utilizan la lectura de código de barras permiten la comprobación manual de los resultados y, por ello, parecen ser las más aptas.

El gran entusiasmo con el que se abrazaron las nuevas tecnologías para fines electorales parece haber sido desplazado por una actitud más cauta, consciente de que las potenciales ventajas del uso de las nuevas tecnologías de nada valen si las garantías del proceso electoral no pueden

ISSN: 1659-2069

asegurarse al ciento por ciento. Por ello, es de esperarse que se continúe invirtiendo en el desarrollo de los sistemas de voto electrónico no conectados a la red. Es probable que hasta que el nivel de debilidades y amenazas de los sistemas conectados a la red disminuyan y de esa manera aumenten las garantías de resultados exactos y sin interferencia ajena, continuará la renuencia a utilizarlos.

REFERENCIAS BIBLIOGRÁFICAS

Bernhard, M. (2017). Public evidence from secret ballot. En *Proceedings E-Vote*-ID 2017 TUT, pp. 121-140. 2nd Joint International Conference on Electronic Voting E-VOTE-ID 2017 24–27 October, Lochau/Bregenz, Austria: Press Tallinn.

Bull, C. et al. (2016). The imperfect storm. En *Proceedings E-Vote-ID 2016* TUT 2016, pp. 116-120. The International Conference on Electronic Voting E-Vote-ID 2016, 18–21 October 2016, Lochau/Bregenz, Austria: Press Tallinn.

Coney, L. (2005). E-Voting: A Tale of Lost Votes. 23 *John Marshall Journal of Computer and Information Law*, 23(3), 509-532.

D'Onofrio, S. (2014). Il voto elettronico. En Riforme, cronache e altri studi Anno accademico 2014-2015, parte prima, pp. 7-18. Sapienza Legal Papers 3. Napoli, Italy: Jovene Editore.

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

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

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

Hamed, E. y Sedky, M. (2016). A High Secured, Cost Effectively E-Voting System. *International Journal of Information Security and Cybercrime* 5(1), 11-31.

Hermanns, H. (2008). Mobile Democracy: Mobile Phones as Democratic Tools. *Politics* 28(2), 74-82.

Lheureux de Freitas, J. et al. (2017). The Brazilian Electronic Voting System: evolution and challenges, pp. 59-71. 2nd Joint International Conference on

ISSN: 1659-2069

Electronic Voting E-VOTE-ID 2017 24–27 October, Lochau/Bregenz, Austria: Press Tallinn.

Loncke, M. y Dumortier, J. (2004). Online Voting: A Legal Perspective. I*nternational Review of Law Computers & Technology* (18), 59-79.

Mercurio, B. (2002). Overhauling Australian Democracy: The Benefits and Burdens of Internet Voting. 21 *University of Tasmania Law Review* 21(2), 23-63.

Mercurio, B. (2004). Democracy in Decline: Can Internet Voting Save the Electoral Process? *John Marshall Journal of Computer and Information Law* 22(2), 409-456.

Pérez, J. (2011). Óbito y resurrección del análisis DAFO. *Revista Avanzada Científica* 14 (2), 1-11.

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

Schwartz, B. y Grice, D. (2013). Establishing a Legal Framework for E-Voting in Canada. *Manitoba Law Journal* (36), 301-418.

Svensson, J. y Leenes, R. (2003). E-voting in Europe: Divergent democratic practice. *Information Polity* 8(1-2), 3-15.

Unt, T., Solvak, K. y Vassil, M.(2016). Family Voting Patterns in E-vote Log Data: Estonian Electronic Elections 2013-2015, pp. 105-107. En *The International Conference on Electronic Voting E-Vote-ID 2016*, 18–21 October 2016, Lochau/Bregenz, Austria: Press Tallinn.

Vinkel, P. y Krimmer, R. (2016). The How and Why to Internet Voting An Attempt to Explain E-Stonia, pp. 239-254. *En The International Conference on Electronic Voting E-Vote-ID 2016*, 18–21 October 2016, Lochau/Bregenz, Austria: Press Tallinn.

Wrede, C. (2016). E-voting in a Small Scale – the Case of Åland, pp. 109-115. En *The International Conference on Electronic Voting E-Vote-ID 2016*, 18–21 October 2016, Lochau/Bregenz, Austria: Press Tallinn.