DOCUMENTO 1 > INFORME DE MAREA GRANATE ACERCA DEL VOTO ELECTRÓNICO

Voto electrónico: Un falso remedio

Carta abierta de Marea Granate a los partidos sobre el voto electrónico y procesos de reforma a la Ley Orgánica del Régimen Electoral General

Desde Marea Granate seguimos, con reacciones encontradas, el Pleno del Congreso de los Diputados celebrado el pasado 20 de abril sobre el establecimiento de una Comisión de Investigación sobre el Voto Rogado. Por un lado, nos satisface el consenso mostrado sobre la necesidad de reformar una ley electoral injusta y antidemocrática. Por otro, somos conscientes de que, al disolverse dicha comisión con motivo de la repetición de las elecciones, todo el respaldo mostrado podría reducirse a pura propaganda electoral. Confiamos, no obstante, en que una vez el parlamento esté en disposición de volver a aprobar la comisión, los partidos políticos reiteren su apoyo a esta, en un ejercicio de buen hacer democrático.

Pero hay algo que nos preocupa aún más que la posibilidad de que todo se quede en agua de borrajas: cómo, una vez más, los portavoces de distintos grupos parlamentarios vuelven a proponer una reforma a puerta cerrada, sin la participación necesaria de los colectivos de españoles en el exterior, que en tanto que afectados directamente son quienes conocen las necesidades y las realidades del voto emigrante.

Fue precisamente esta forma de actuar la que nos trajo a la situación actual, con la introducción del sistema de ruego del voto tras la aprobación de la LOREG en 2011. La falta de atención (o voluntad política) a la hora de estudiar las potenciales consecuencias de la implantación del voto rogado introdujo una serie de problemas a día de hoy se siguen manifestando en un **alarmante descenso del 85% en las tasas de participación** desde la introducción de la reforma. Un descenso que, además, resultaba previsible y fue anticipado por un informe de la Junta Electoral, que advertía de porcentajes similares de participación electoral en los procesos municipales, donde ya se había impuesto el ruego del voto.

Su unilateral “solución” es, en esta ocasión, la implantación de un sistema de voto electrónico. Marea Granate solicita a los partidos políticos, por tanto, un gesto de responsabilidad política para evitar que se lancen de nuevo irreflexivamente a la imposición de un sistema que ha demostrado repetidamente su nula fiabilidad y auditabilidad. Los sistemas de voto electrónico han sido fundadamente rechazados por países como Alemania, Inglaterra o Noruega. Reiteramos, una vez más, que la necesaria y urgente reforma electoral ha de acometerse teniendo en cuenta las realidades del voto exterior, en

diálogo abierto con las personas (emigrantes) implicadas y los colectivos en los que se organizan. Adicionalmente, proponemos soluciones viables, seguras y más económicas para garantizar el acceso al derecho al voto de todos las y los españoles residentes en el extranjero.
Es necesario precisar que el presente documento se refiere exclusivamente al voto electrónico; Marea Granate continúa abogando por que los trámites consulares puedan ser realizados a distancia, ya que son procedimientos más simples, con menores riesgos y con un interés menor en ser interferidos; al contrario que en un proceso electoral, donde la complejidad es enorme, los riesgos numerosos y los potenciales intereses de modificar el resultado evidentes.

Voto electrónico: Un falso remedio

La propuesta de un sistema de voto electrónico como solución estrella a nuestros problemas de participación política es un producto de marketing muy potente: España entra en el futuro, en la vanguardia tecnológica. Desde Marea Granate, sin embargo, nuestras exigencias son aquellas de soluciones reales a problemas reales.

En el ámbito electoral, venimos denunciando desde hace tiempo cómo la violación de nuestro derecho a voto, demostrada de facto por la una alarmante caída en la participación de un 85%, se produce tras la introducción de la Ley Electoral de 2011 y por una serie de trabas que incluyen las distancias a consulados, problemas en el censo y las inscripciones y papeletas que no llegan a tiempo.

El término de voto electrónico es vago e incluye dos modalidades, a cual más indeseable que la anterior. Por un lado, puede referirse a la sustitución de las urnas de cristal por urnas electrónicas (léase ordenadores) en los consulados. Sin necesidad de incurrir en un análisis de seguridad de un tal sistema, demostrado como desastroso en numerosas ocasiones (véase más abajo), ¿en qué soluciona esto nuestros problemas, mientras el calendario, las distancias a los consulados, y sus horarios son los mismos? ¿O cuando no te has podido inscribir en el censo para votar?

La otra posible categoría es aquella del voto por internet, es decir, emitido a través de la red desde cualquier dispositivo en propiedad del votante. Aunque esto pueda resultar a primera vista una posibilidad teórica, con varios grupos de investigadores de diversas disciplinas trabajando en ella, esto no implica que sea **factible** en la práctica a día de hoy.

(In)viabilidad: Análisis técnico

Nos preocupa, por encima de cualquier otro aspecto y en tanto que primera condición necesaria, la viabilidad técnica de un sistema **seguro** de voto electrónico a través de internet. Todo proceso electoral debe ser auditable públicamente, de forma que no quepa ninguna duda sobre el resultado final. Sin dichas garantías, sin saber si se ha producido una modificación arbitraria del resultado de las elecciones, lo que se introduce en realidad es **una reforma antidemocrática.**

Las cuatro propiedades exigidas a un sistema de voto son las siguientes:

Accesibilidad: Todos los votantes autorizados han de tener una oportunidad real de votar.
Integridad: Ha de asegurarse que cada votante pueda verificar que su voto emitido ha sido contabilizado en el recuento final, y que éste no ha sido modificado durante el proceso.
Secreto del voto: Nadie puede ser capaz de asociar a un votante con un voto. Ni siquiera el propio votante puede demostrar a quién voto, para evitar coerciones.
Autenticación del votante: Sólo los votantes autorizados pueden votar, y solamente el número de veces estipuladas.
El voto por internet multiplica todos los riesgos de un sistema de voto no presencial, al requerir prácticamente el mismo esfuerzo atacar a un voto o a dos millones. Errores introducidos maliciosamente o por descuido, virus informáticos y omisiones imprevistas pueden romper las propiedades arriba expuestas, y para ello sólo es necesario la colaboración o el descuido de un individuo o un pequeño grupo de ellos. Peor todavía, mientras que en el equivalente físico hacen falta muy pocas personas para detectar y denunciar un fraude, en el caso digital la detección es muchísimo más complicada, o incluso imposible en la mayoría de las ocasiones.

Delegar nuestro voto y nuestra confianza en estos sistemas electrónicos no resuelve los problemas de nuestra ya injusta ley electoral actual, sino que los multiplican.

Problemas de Accesibilidad

Aunque el requisito de **Accesibilidad** pudiera parecer a priori ajeno a la categoría de seguridad, desalentar o en última instancia imposibilitar el ejercicio del derecho a voto a determinadas personas, poseedoras de una intención de voto distinta a la del atacante, es un ataque real y que venimos sufriendo y denunciando a lo largo de estos años.

Un sistema de voto a través de internet introduce riesgos en la Accesibilidad no sólo por el sesgo demográfico de los votantes que utilizarían tal sistema, sino principalmente mediante ataques de denegación de servicios (DoS, de las siglas en inglés Denial of Service). Hay dos razones por las cuales es necesario protegerse ante tales ataques: En primer lugar son los más sencillos de perpetrar contra cualquier objetivo dentro de la infraestructura, y son en general tan rutinarios en internet que existen negocios ilegales online que pueden conducir un ataque contra el objetivo de tu elección por un precio moderado. No estamos haciendo aquí un ejercicio de imaginación: Ataques distribuidos de denegación de servicios (DDoS) ya han sido utilizados en elecciones públicas reales a lo largo del mundo, y han sido publicados en al menos en cuatro ocasiones (Arizona Democratic Primary, 2000; Ontario New Democratic Party, 2003; Hong Kong people’s election, 2012; New Democratic Party of Canada 2012) [1].

Peor aún, la denegación de servicios se puede producir desde el propio ordenador del votante, mediante su infección con malware: El virus informático podría hacer parecer al votante que se ha producido un error, lo que llevaría al votante medio a culpar a su proveedor de internet, su “chatarra” de ordenador, o un ataque de denegación de servicio generalizado. O hacer parecer que el voto se ha realizado correctamente, cuando no es el caso.

Decimos, en este caso, peor aún, porque esto permite realizar dicho ataque **de forma selectiva**: Quien escribe el malware probablemente quiera saber la intención de voto del votante antes de decidir si bloquear o no su derecho a voto. Desgraciadamente, tanto en el ordenador como el teléfono móvil de un usuario hay muchas pistas y evidencia al respecto, y algo tan simple como acceder al historial de navegación puede ser suficiente para que el atacante descubra el/los partido(s) preferido(s) o la clase social del votante. No necesita más.

Algunos votantes podrían estar lo suficientemente educados en seguridad informática como para detectar estos problemas, si hubiera como sería necesario mecanismos adecuados de verificación tras el recuento, pero: ¿Cómo podría probar a la autoridad electoral que realmente trató de votar, pero un virus informático se lo impidió?

A día de hoy, no existe una solución contra ninguno de estos ataques de denegación de servicios, que podrían dejarnos sin votar de nuevo a gran parte del electorado.

Ataques a la Integridad y/o Secreto del Voto

Todo proceso electoral debe ser auditable públicamente, de forma que no quepa ninguna duda sobre el resultado final. Fue por este motivo, el sistema de voto electrónico fue declarado inconstitucional en Alemania en 2009 [3]. En teoría, un sistema de voto electrónico podría desplegarse mediante un software de código abierto, al que todo el mundo tuviera acceso para auditar su seguridad, y con un largo historial de uso. Sin embargo, una y otra vez, se delega esta labor en empresas privadas que, con la excusa de un modelo de negocio basado en la propiedad intelectual, proporcionan software de código cerrado, dificultando la tarea de analistas de seguridad imparciales.

Preocupa, por tanto, que la seguridad de un proceso dicho democrático repose de facto en un grupo reducido de personas con acceso al desarrollo, ejecución y evaluación de los sistemas. Mientras tanto, el resto del electorado pasa a ser ciudadanos de segunda.

¿Cómo podemos estar seguros de que este código e infraestructuras opacas, a los que tienen acceso un grupo muy reducido de personas, son seguros? ¿Podemos arriesgarnos a esperar que un analista de seguridad de buena voluntad encuentre y publique los fallos antes de que lo haga cualquier otro individuo o grupo con intenciones de modficar el resultado de las elecciones? En el caso de que lo hiciéramos, ¿podemos afirmar que los errores serían detectados con un margen de tiempo razonable para ser corregidos?.

¿Cómo garantizar que el software que se encuentra en una máquina especializada frente a nosotros, el día de las elecciones, no ha sido modificado para alterar nuestro voto? O en el caso de votar por internet desde cualquiera dispositivo, ¿cuáles son las garantías de que nuestro ordenador, o el de otro de los votantes, no está infectado para modificar o simular ese programa, pero de una forma maliciosa? Una pista para esta última pregunta: un antivirus está lejísimos de ser una solución suficiente.

El recuento final

Por si esto fuera poco, el sistema informático encargado de realizar el recuento final y transmitirlo para su publicación es el único que se necesita comprometer para modificar el resultado de las elecciones. Si, en un escenario de ciberguerra abierta como en el que vivimos, Estados Unidos e Israel lograron parar una central nuclear Iraní [4], ¿a qué posible enemigo de nuestra soberanía representativa no le interesaría vulnerar nuestros resultados electorales de forma imperceptible?

(In)viabilidad: Aspectos económicos

Un falso pero común argumento a la hora de defender los sistemas de voto electrónico es aquel del coste de su despliegue. Sin embargo, el coste del despliegue de sistemas **inseguros** (ver análisis técnico arriba) de voto electrónico en el pasado varía entre el millón y medio de dólares y las decenas de millones [1]. Siendo este el precio para sistemas **inseguros**, es más que razonable esperar que, aunque la tecnología llegara a evolucionar lo suficiente en las próximas décadas, crear e implementar un sistema de voto por internet garantista y verificable de extremo a extremo costaría varias decenas de millones de euros. Aunque este no sea el argumento principal, nos hace observar con mayor escepticismo si cabe a aquellas personas que proponen sistemas de este tipo bajo un argumento de ahorro: Si no se trata de ignorancia, sus intereses económicos o políticos personales de desarrollar sistemas inseguros son realmente preocupantes.

(In)viabilidad: Aspectos legales

Tras la exposición de todos estos problemas, queda como cuestión abierta a dirimir si el marco legal español permite tan siquiera el uso de sistemas de voto electrónico en el escenario de unas elecciones generales. En Noruega fue descartado tras dos pruebas piloto en 2014, dado a las pocas garantías de seguridad que ofrecía a los votantes, y la falta de impacto en aumentar el número de votantes [5]. En Alemania, en 2009, fueron más concluyentes: Tras la denuncia por parte de colectivos sociales ante la irresponsabilidad y vulnerabilidad de los sistemas de voto electrónico, éstos fueron declarados inconstitucionales [3], dejando el problema zanjado.

Lecciones históricas: Fiascos reales

Existen numerosos casos que ilustran la inviabilidad del voto electrónico, así como casos de países que han desistido de su implementación, ya sea por sentencias legales, como en el caso alemán, o por estudios encargados por el propio gobierno a comisiones expertas, como en el caso de Noruega o de Inglaterra. Los casos más conocidos de interferencias no deseadas (hackeos) y vulnerabilidades existentes en sistemas de voto electrónico son:

- **Sudáfrica:** 1994, primeras elecciones post-apartheid. La única parte del proceso llevada a cabo de forma electrónica era el recuento (escrutinio). Peter Harris descubrió que se había vulnerado la seguridad de la red para multiplicar los votos de ciertos partidos opuestos al CNA. Dado que el sistema no era puramente electrónico, se pudo contrarrestar el ataque contando manualmente los votos (lo que

ralentizó considerablemente el escrutinio). El ataque cibernético no se hizo público entonces para evitar revueltas.

- **Irlanda** llevó a cabo un ensayo de voto electrónico en 2002. En 2006, un grupo de hackers neerlandeses, liderados por Rop Gonggrijp, demostraron cómo se podía vulnerar el sistema [22]. Irlanda anunció oficialmente su rechazo a estos medios en 2009.
- **Estados Unidos de América:** 2004, elecciones ganadas por Bush. DIEBOLD, INC. El resultado de estas elecciones aún queda en entredicho, por manipulación deliberada del conteo de votos, con la exclusión del voto proveniente de población afroamericana y latina.
- **Reino Unido**: En 2008 y tras una treintena de pruebas piloto, la Comisión Electoral encargada del informe sobre el voto electrónico, declaró que este no ofrecía las suficientes garantías para poder ser aceptado y en consecuencia, se descartó como método electoral.
- **Finlandia:** En el miso año, a las y los fineses le bastó un ensayo para abandonar los sistemas de voto electrónico. Este se llevó a cabo en 3 municipios, en los cuales 232 votantes vieron su voto desaparecer del recuento final. Como resultado, se repitieron las elecciones. Más información puede encontrarse en el informe de la Electronic Frontier Finland [20].
- **Alemania:** El voto electrónico fue puesto a prueba en Alemania entre 1999 y 2008. El Chaos Computer Club de Alemania y el grupo “Wij vertrouwen stemcomputers niet” de Países bajos analizaron las máquinas muy similares a las utilizadas en Alemania y lograron romper su seguridad en 2006 [16]. El voto electrónico fue declarado inconstitucional en 2009 por conflicto con la auditoría pública: *German constitutional court decision to declare the use of voting machines unconstitutional* [3].
- **Ucrania:** En 2014, el ataque cibernético por parte de personas afines a Rusia tuvo por objetivo desacreditar el proceso electoral, interrumpiendo el escrutinio y causando que el sistema produjera resultados incorrectos. [6].
- **Bélgica:** La historia de fraudes (o incoherencias, a ojos del lector queda) es larga, con máquinas en las que han aparecido miles de votos de origen desconocido o incoherencias en el recuento final [19].
- **Buenos Aires, Argentina:** 2015 Las máquinas de lectura de los votos electrónicos eran manipulables por los usuarios de modo que era posible cambiar al configuración de la pantalla táctil de forma que el elector votaba de hecho a un candidato distinto al elegido. [8,9] Los hechos fueron, de nuevo, silenciados, y han sido hechos públicos a través de la Fundación Vía Libre [15].
- ¿Voto desde casa y por internet? **Estonia**, es prácticamente el único país que mantiene este sistema en sucesivas elecciones, aunque un grupo de investigadores de la universidad de Michigan, encontró que el sistema de voto por Internet presentaba serias limitaciones en su diseño y fallos en su implementación que ponian en peligro la integridad de las elecciones [10].
- Tras varios ensayos, **Australia** rechazó el voto electrónico a nivel federal. El informe final del Parlamento Australiano, motivado por los fallos de seguridad detectados durante las elecciones de 2013, fue publicado en 2015, con un mensaje muy claro: “El Comité ha analizado los riesgos y beneficios asociados con procesos electorales electrónicos, tanto en Australia como internacionalmente. Hemos concluido que introducir un sistema de voto electrónico a gran escala en un futuro próximo

comprometería peligrosamente la integridad de las elecciones federales" [17, Foreword, Página x, párrafo 4]. Caber rechazar la insistencia, a pesar de las numerosas evidencias y el rechazo a nivel federal, la insistencia en New South Wales por seguir usando el sistema de voto por internet conocido como iVote, desarrollado por la empresa barcelonesa Scytl, que se ha ido utilizando desde 2010 a pesar de sus repetidas vulnerabilidades. La última de ellas fue descubierta y publicada en Marzo de 2015 por J. Alex Halderman y Vanessa Teague [18]: Los investigadores insisten en el enorme riesgo de estos sistemas, como queda patente por el tiempo que la vulnerabilidad estuvo activa, en pleno proceso de emisión de votos, hasta que ellos la encontraron y pidieron corregir. ¿Y si el error lo hubiera encontrado alguien con distintas intenciones?

- **India:** En 2010, Hari Prasad junto con J. Alex Halderman denuncian y demuestran que las "EVMs" (máquinas de voto electrónico) de India son inoperantes y vulnerables en numerosos puntos con gravísimas consecuencias [21]. Lejos de buscar soluciones, el gobierno indio negó la existencia de problemas y por el contrario, castigó a los delatores: Hari Prasad fue detenido y pasó 7 días bajo custodia policial; Halderman fue deportado a su llegada a la India.En 2014, el Estado de Guyarat utilizó las máquinas de voto electrónico remoto (a través de internet) de Scytl. Exacto, la misma compañía que se encargó del sistema iVote de New South Wales en Australia. Con el mínimo margen de tiempo entre ambas elecciones, cabe la duda de que ambas elecciones no utilizaran exactamente las mismas máquinas y protocolos criptográficos. ¿Fue el completo de los votos emitidos en Gujarat, entonces, tan vulnerable como se detectó luego a mitad de los comicios australianos?
- **Francia** se suma los países que han tenido que sufrir el despliegue de un sistema inseguro por parte de Scytl y Atos [13].
- **Noruega** se suma a los países que tras un largo periodo de trabajo de grupos expertos, han descartado el uso del voto electrónico como método electoral dadas las escasas garantías ofrecidas por dicho método y la gran cantidad de potenciales ataques a los que podría ser sometido el sistema electoral con consecuencias desastrosas.
- **Brasil** es otro de los países con una historia tan larga como desastrosa de sistemas de voto electrónico, con sistemas poco auditables y máquinas vulnerables [11].
- **Israel** [12].

La lista podría continuar. Nos resulta especialmente preocupante un denominador común en muchos de estos casos y en el que quizás no hemos insistido lo suficiente: A aquellas personas que denunciaron una vulnerabilidad en estos sistemas, en la mayoría de las ocasiones no sólo no se las escuchó ni se trató de seguir su consejo para corregir errores, retirar el sistema, o parar las elecciones, sino que se las trató de silenciar lo máximo posible. Analistas de seguridad y figuras del mundo académico fueron consideradas como criminales, enemigas, o traidoras a la patria, incurriendo incluso en penas de prisión [2].

Conclusión

No todo lo nuevo es necesariamente bueno. En la era digital, determinados trámites son, para ventaja de los usuarios, procesables desde sistemas telemáticos —tales como el registro consular, la comunicación de cambio de domicilio o el propio ruego del voto. En

estos procesos el interés particular de saboteo o intereferencia es mucho menor, y además el propio usuario tiene la posibilidad de comprobar que el procedimiento ha cumplido con su propósito (por ejemplo, llamando al consulado para comprobar que sus datos han sido correctamente recibidos). El caso del voto electrónico es diferente por dos razones: primera, porque sí que existe un potencial y enorme interés por interferir en la voluntad y el propósito del proceso (cambiar el resultado electoral modificando los votos de quienes lo ejercen) y segunda, porque no existe la posibilidad de comprobar que el proceso ha cumplido su función (el voto emitido y escrutado coinciden y son el deseado). Además de esto, el grado de vulnerabilidad en términos del número de posibles votos secuestrados es mucho mayor [1, 7] que en los sistemas de voto físico, en urna, y los de voto postal, que tienen siglos (décadas en el caso postal) de historia, tiempo durante el cual han podido ser refinados para resistir a la mayoría de los ataques concebibles y, sobre todo, a aquellos a gran escala.

Ante el problema del ejercicio de nuestros derechos como emigrantes, hace falta un análisis riguroso, serio y responsable de la realidad y los medios y, a partir de ahí, sopesar soluciones. Ninguna ley electoral que vuelva a escribirse sin la participación de la sociedad civil y aquellos expertos (sin intereses económicos en la implantación de determinadas propuestas) que conocen la problemática del voto telemático y emigrante podrá incurrir en una solución.

Por ello, en tanto que afectadas directamente por estas leyes y tras exponer lo inseguro, inviable y por lo tanto antidemocrático de una propuesta de voto electrónico para acabar con el voto rogado, desde Marea Granate insistimos:

El voto electrónico no es una solución viable en nuestros días, sino una vulneración que ataca a nuestra soberanía en los comicios electorales.

Y recordamos nuestras propuestas para reformar la Ley Orgánica del Régimen Electoral General de 2011 que introdujo el voto rogado:

1.- Reforma de la ley electoral, en estrecha colaboración con los colectivos ciudadanos: Derogación del voto rogado, ampliación de los plazos de envío de la documentación y de los mecanismos para efectuar dichos envíos; desde Marea Granate apostamos por el uso de diversos sistemas en paralelo que garanticen el derecho a voto de todos los emigrantes:

1) Voto por correo, aumentando los plazos de envío y recepción de papeletas y proporcionando métodos alternativos que garanticen el acceso a la documentación electoral, como la descarga telemática de las papeletas.

2) Depósito de voto en urna en el consulado, mejorando la seguridad de custodia de las urnas e implementando un sistema de trazabilidad del voto. Actualmente, las urnas permanecen hasta 72h sin una correcta custodia, pudiendo llegar hasta cinco días extraordinariamente, como en las elecciones del 20 de diciembre de 2015. Este hecho fue denunciado con anterioridad por la Junta Electoral Central sin que se hayan tomado medidas al respecto. [14]

3) Voto por procuración, siguiendo modelos como el francés.

2.- Implantación de un sistema de inscripción a distancia y de reclamaciones del censo electoral que elimine los problemas de acceso por horarios y distancia a los

consulados. Avance en la informatización del sistema de gestión del censo electoral, para garantizar la correcta actualización de inscripciones y cambios de domicilios.

3.- Establecimiento de una circunscripción exterior que dé a la emigración el peso político que le corresponde.

4.- Mejora de la información institucional. Campañas informativas con medios y antelación suficiente, adecuada formación del personal consular y canales de consulta eficaces. Transparencia en los escrutinios y reclamaciones y gratuidad del voto.

5.- Adecuación de recursos humanos y tecnológicos proporcional al volumen de personas emigradas.

[1] Overseas Vote Foundation. The future of voting: End-to-end verifiable internet voting specification and feasibility assessment study. https://www.usvotefoundation.org/news/E2E-VIV-press, 2015.

[2]https://freedom-to-tinker.com/blog/jhalderm/electronic-voting-researcher-arrested-over-anonymous-source/

[3] BVerfG, 2 BvC 3/07 vom 3.3.2009, Absatz-Nr. (1-163). Available at http://www.bverfg.de/entscheidungen/cs20090303_2bvc000307.html (9.10.2011). The core of the decision in German: *"Der Grundsatz der Öffentlichkeit der Wahl aus Art. 38 in Verbindung mit Art. 20 Abs. 1 und Abs. 2 GG gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen. Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können."*

[4] http://www.elladodelmal.com/2013/01/incidentes-de-ciberguerra-y.html

[5] Internettvalg – Hva gjør og mener velgerne? https://www.regjeringen.no/globalassets/upload/KMD/KOMM/rapporter/ISF_Internettvalg.pdf , 2014.[6] M. Clayton. Ukraine election narrowly avoided 'wanton destruction' from hackers. Christian Science Monitor, June 2014. http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video

[7] Real-world Electronic Voting: Design, Analysis and Deployment (Series in Security, Privacy and Trust). Ataques reales no capturados por los modelos teóricos pueden leerse aquí http://eprint.iacr.org/2016/447.pdf y ataques reales a implementaciones reales, aquí: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

[8] https://www.eff.org/node/86911

[9] http://www.elladodelmal.com/2015/07/como-votar-multiples-veces-con-el.html

[10] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

[11] http://www.zdnet.com/article/fraud-possible-in-brazils-e-voting-system/

[12] http://iss.oy.ne.ro/e-Voting-RFID-Relay-IEEE.pdf

[13]http://www.numerama.com/magazine/22687-vote-par-internet-il-faut-utiliser-un-ordinateur-qui-n-est-pas-a-jour.html

[14]http://www.lavozdegalicia.es/noticia/galicia/2014/04/03/junta-electoral-lamenta-gobierno-siga-dar-garantias-voto-emigrante/0003_201404G3P11992.htm
[15] http://votoelectronico.org.ar/
[16] https://berlin.ccc.de/wiki/Wahlmaschinen
[17]http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Final_Report
[18] https://freedom-to-tinker.com/blog/teaguehalderman/ivote-vulnerability/
[19]http://www.cio.com/article/2376004/e-voting/software-bug-disrupts-e-vote-count-in-belgian-election.html
[20] https://effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf
[21] https://indiaevm.org/evm_tr2010-jul29.pdf
[22] Nedap/Groenendaal ES3B voting computer a security analysis
http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

ANEXOS

- **Voto por internet. El caso Estonio:**

  VÍDEOS:
  - https://www.youtube.com/watch?v=eW296J2Qfms&feature=youtu.be (subtitulado en español)
  - https://www.youtube.com/watch?v=PT0e9yTD2M8

  ESTUDIO TÉCNICO DEL CASO:
  - https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

- **Recopilación de noticias acerca de los casos de Scytl en el extranjero:** Francia, India, New South Wales (Australia), Ecuador, México, EEUU, Canadá:

  - New South Wales (Australia) > máquinas posteriormente utilizadas en India: https://arxiv.org/pdf/1504.05646v2.pdf (estudio técnico) http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Final_Report https://freedom-to-tinker.com/blog/teaguehalderman/ivote-vulnerability/
  - EEUU, Canadá, etc.: https://digitalvote.wordpress.com/2014/03/07/scytl-compromises-credibility-of-the-voting-technology-industry/
  - Ecuador: http://e-lected.blogspot.dk/2014/03/scytl-fails-again-in-ecuador.html
  - Francia: http://www.numerama.com/magazine/22687-vote-par-internet-il-faut-utiliser-un-ordinateur-qui-n-est-pas-a-jour.html http://elections.lefigaro.fr/presidentielle-2012/2012/05/24/01039-20120524ARTFIG00676-bugs-en-serie-pour-le-vote-par-internet-des-expatries.php

OTROS CASOS:

- Noruega no ha implanta el voto electrónico: https://thevotingnews.com/governments-should-consider-the-consequences-when-they-decide-whether-to-adopt-internet-voting-democratic-audit-uk/
- Voto electrónico en Canadá, no recomendado: https://en.wikipedia.org/wiki/Electronic_voting_in_Canada https://papervotecanada2.wordpress.com/
- Polémicas de voto electrónico en Bélgica. http://www.poureva.be/?lang=fr
- Problemas del voto electrónico en USA: https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf