Universidad de León

Departamento de Ingeniería Eléctrica y de Sistemas y Automática

Desarrollo de una metodología para el análisis y la clasificación de los sistemas de voto electrónico

Tesis doctoral dirigida por el
Dr. Don Justo Carracedo Gallardo y
el Dr. Don Ángel Alonso Álvarez

Luis Panizo Alonso

León, diciembre de 2014

Dedicatoria

Esta tesis doctoral está dedicada a mis padres, a mis hijos y a mi paciente compañera Silvia.

“Las cosas deben ser tan sencillas como sea posible, pero no más”.

Atribuido a Albert Einstein

.

Agradecimientos

En primer lugar quiero mostrar mi mayor agradecimiento a D. Justo Carracedo Gallardo y a D. Ángel Alonso Álvarez, directores de esta tesis doctoral, ya que sin su orientación y apoyo no hubiera sido posible.

También quiero agradecer a todas las personas que me han ayudado y alentado a la hora de elaborar esta tesis, pero me gustaría hacer mención especial de:

Muy especialmente a Jorge Ramió y a Emilia Belleboni por sus múltiples y acertadas correcciones.

A mis compañeros Javier Alfonso, Héctor Aláiz, Ramón Ángel Fernández, Manuel Alija, Ángela Díez y Mª José Álvarez por su ayuda.

A mis amigas Eva Méndez y Teresa Llamazares por su valiosas opiniones.

Espero que el trabajo realizado sea merecedor de toda la ayuda recibida.

Antecedentes

La presente tesis doctoral se ha redactado en el periodo que va desde marzo de 2012 a noviembre de 2014.

En realidad su génesis comenzó en abril de 2002 cuando se creó, dentro de la Universidad de León, el O.V.E. (Observatorio de Voto Electrónico) del que el autor fue miembro fundador y secretario general. Posteriormente se desarrollaron seis congresos internacionales sobre voto electrónico, pioneros en España, denominados Votobit. Los dos primeros en León [1] y los siguientes en México (Coahuila y Nuevo León), Argentina y Perú. En todos ellos fui ponente.

Paralelamente actué de observador internacional de procesos electorales con urnas electrónicas en México, Venezuela, Argentina, Francia y Perú.

Previamente a esta tesis he publicado varios documentos y artículos sobre el tema:

- Aspectos tecnológicos del voto electrónico. Oficina nacional de procesos electorales de Perú. 2007. http://hdl.handle.net/10612/3139 [2].
- Technological solutions for electronic voting and guarantees of the integrity of the electoral process. A case study. 2010 http://hdl.handle.net/10612/2845 [3].
- Aspectos tecnológicos del voto electrónico. Capítulo del libro *Democracia digital, participación y voto electrónico* de la Fundación CEPS. 2010. http://hdl.handle.net/10612/3144 [4].
- Technical audit of an electronic polling station: a case study. International Journal of e-services and mobile applications. 2011. http://hdl.handle.net/10612/3142 [5].
- Libro blanco sobre el voto electrónico. Plataforma votoe.es. 2013. http://hdl.handle.net/10612/3145 [6].

Resumen

El trabajo realizado en esta tesis doctoral ha consistido en:

- Estudiar la documentación relacionada con los procesos y soluciones en el entorno de la votación electrónica que se han publicado hasta el comienzo de la redacción de esta tesis (marzo de 2012).
- Analizar las últimas soluciones que en el entorno académico se han propuesto para dar solución al problema de las auditorías en el ámbito de la votación electrónica presencial y, concretamente, con los denominados sistemas de votación auditables de extremo a extremo (*End-to-end auditable voting systems*).
- Comparar todas las soluciones propuestas desde diversos puntos de vista con la dificultad añadida de que algunos de ellos no han sido utilizados en la práctica.
- Redactar las conclusiones sobre lo que aportan cada una de las soluciones analizadas de forma individual y conjunta en el ámbito de los procesos presenciales de votación electrónica.

Abstract

The aim and scope of this thesis describes:

- The study of documentation related to the processes and solutions in the context of electronic voting published up to this moment. (March 2012).
- Up to date analysis of the latest solutions developed by recent research and scholarship in the field of presential electronic voting and more specifically with end-to-end auditable voting systems.
- To compare proposed solutions from different points of view with the additional difficulty that some of them have not been put into practice yet.
- The final conclusions provide solutions for each of the proposals and as a whole in the field of the processes of the presential electronic voting

Índice de contenido

Capítulo 1

Capítulo 2

Capítulo 3

Capítulo 4

Capítulo 5

Referencias

Índice de figuras

Índice de tablas

Índice de expresiones

Auditoría "Proceso sistemático, independiente y documentado para la obtención de registros, hechos o cualquier otra información relevante, con el fin de evaluarlos de manera objetiva y poder determinar el grado de cumplimiento de los requisitos especificados". Definición de VVSG en 2005.

Bulletin board Tablón de anuncios digital en el que se publica información de un proceso electoral con el fin de poder comprobar algún aspecto de los votos emitidos.

Cifrado homomórfico (homomorphic encryption)
Cifrado que permite que se pueda calcular la suma de dos números sin tener que descifrar los mismos. Se puede utilizar en sistemas de verificación del voto ya que el votante puede publicar su voto cifrado sin revelar el voto en sí, y la suma de los votos se puede calcular sin conocer el voto de cada votante.

Coacción (Coercion) Cualquier tipo de acción ilegal para influir sobre un votante y que implica conocer como ha votado.

Comprobar o verificar "Pasar a tener la certeza de la veracidad de una suposición, un dato o un resultado obtenido anteriormente mediante demostración o pruebas que los acreditan como ciertos." DRAE.

DRE (direct-record electronic, direct recording electronic)
Equipo que permite emitir, registrar y contabilizar votos por medios electrónicos. Es un tipo de urna electrónica.

EAC (Election Assistance Commission) Comisión federal de los EE.UU. para supervisar los procesos electorales.

EVM (Electronic voting machine) Otra denominación de **DRE**.

E2E (verificación de extremo a extremo (end to end))
También denominada por el autor **verificación indirecta mediante recibo.** En general este tipo de comprobación permite que tanto el votante, al final del proceso electoral, verifique que su voto ha sido contabilizado, como que pueda realizarse una comprobación general sobre todos los votos emitidos. VVSG 2007.

E-petitions Proceso de participación ciudadana que permite enviar solicitudes a las autoridades por parte de los ciudadanos, mediante una plataforma conectada a Internet.

HAVA (Ayuda a América a votar) Ley promulgada en el 2002 en los EE.UU. para mejorar los procesos electorales.

Método Mercuri (Mercuri method) Un método de votación, popularizado por la investigadora Rebecca Mercuri, en el que el votante tiene la oportunidad de ver su voto en papel al mismo tiempo que se registra en la urna electrónica. La papeleta generada con su voto se deposita de forma automática y sin intervención del votante en una urna convencional, por si fuera necesario comprobar el resultado del recuento electrónico.

OCR Lector o escáner óptico de caracteres o marcas depositadas sobre un papel especialmente diseñado para ello.

Optically scanned ballot Papeleta de votación para lectura óptica mediante OCR.

OVE Observatorio Voto Electrónico de España.

Papeleta desafío Una papeleta de votación no vinculante que se puede utilizar antes de la votación real con objeto de verificar que el proceso de votación es fiable.

Papeleta mariposa (butterfly ballot) Una papeleta de dos páginas en la que las opciones a votar están en una única columna central y cuya escasa usabilidad propició importantes problemas y errores a los votantes del Condado de Palm Beach, Florida, en la carrera presidencial de los EE.UU. en el año 2000.

PCOS Equipo para la votación electrónica compuesto de un lector óptico de papeletas (OCR) que permite comprobar que la lectura del voto es válida y en este caso la papeleta es depositada automáticamente en la urna; en otro caso es rechazada. Opcionalmente puede disponer de una impresora para generar un recibo para la verificación posterior del voto emitido.

PKI Infraestructura de clave pública que permite el desarrollo con garantías de operaciones de cifrado.

PRNG Generador de números pseudo-aleatorios.

Protocolo de conocimiento cero (zero-knowledge proof) Un protocolo nada intuitivo por el cual somos capaces de demostrar que un enunciado es verdadero sin revelar ninguna información sobre el mismo salvo que es cierto. Las pruebas de conocimiento nulo son importantes en una serie de esquemas de votación criptográficos, ya que permiten al sistema demostrar que se ha registrado un voto correctamente sin revelar información sobre el mismo.

Protocolo de redes de mezcla (mixnets) Es un protocolo criptográfico que ejecutado por un conjunto de servidores denominados de mezcla, proporciona el anonimato para un mensaje enviado, siendo imposible localizar su fuente. El mensaje individual puede ser cifrado y mezclado de forma que después del proceso de descifrado no es posible determinar quién fue el remitente del mensaje. En el caso de la votación electrónica consiste en hacer públicas las papeletas sin poner en peligro la anonimia de los votantes.

Recibo anti-coacción (freeness receipt) Documento en papel que se emite en el momento de la votación para que el votante pueda comprobar que su voto ha sido contabilizado, pero que impide demostrar qué se ha votado.

Recibo de verificabilidad del voto (voter-verified audit trails) Recibo que emite una urna electrónica con el objeto de permitir comprobar que el voto ha sido contabilizado.

Sistema de votación electrónica (Electronic voting system) Sistema de votación que involucra el proceso de elección, depósito del voto y de contabilización de los mismos por medios electrónicos.

Smart-card Tarjeta que contiene un circuito integrado en el que se almacena información para ser leída con un dispositivo externo.

TCP/IP Familia de protocolos de comunicaciones utilizados por Internet.

TIC Tecnologías de la Información y de las Comunicaciones.

TRNG Generador fiable de números aleatorios.

Urna electrónica Equipo electrónico que permite recoger un voto por algún medio electrónico y que ha sido diseñado y construido con ese fin. Puede estar conectada a la red (modo on-line) o no (modo off-line). Pueden ser de diversos tipos, como las de lectura óptica mediante OCR o de tipo DRE.

Usabilidad (usability) Según la ISO 9421 es la "eficacia, eficiencia y satisfacción con la que un conjunto específico de usuarios puede alcanzar un conjunto específico de tareas en un entorno particular". En el contexto del voto electrónico se refiere a "la capacidad de los votantes para emitir votos válidos, de forma rápida, sin errores y con la confianza de que su elección se ha grabado correctamente". VVSG, 2007.

VE (e-voting) Votación electrónica.

VoComp Conferencia-competición sobre sistemas de votación electrónica diseñados por universidades que se celebró en el 2007 en Portland, Oregon.

Votación con auditoría abierta (open audit voting) Sistema de votación electrónica que aporta algún tipo de solución abierta (no dependiente de fabricantes) para verificar en todo o en parte el proceso electoral.

Votación por Internet (i-voting) Votación electrónica utilizando Internet.

Votación telemática (Remote electronic voting o REV) Proceso de votación que puede realizarse desde cualquier lugar físico en el que se disponga del dispositivo electrónico adecuado, bien sea un ordenador, un teléfono móvil, agendas electrónicas, etc. Algunos autores lo denominan **votación electrónica remota** que sería equivalente.

Voter-verifiable Sistema que permite al votante la comprobación total o parcial del proceso electoral.

Voter verification "Acto por el que un votante puede comprobar por sí mismo que su voto ha sido registrado y contabilizado correctamente, así como que todos los votos fueron registrados tal y como los votantes lo habían previsto." VVSG, 2007.

Voto electrónico (e-voto) Voto emitido mediante un equipo digital y que es recogido y contabilizado por ese medio informático.

Voto en cadena (chain voting) Conocido fraude que se puede realizar sobre una urna electrónica que permita el acceso físico a la papeleta emitida por la misma para ser depositada en una urna convencional con objeto de poder desarrollar una comprobación posterior de los votos emitidos (caso de Venezuela y México). Para ello se entrega al votante una papeleta previamente marcada con una determinada selección y una señal adicional que la hace única; posteriormente entra en el lugar de votación y emite otra papeleta idéntica, pero deposita en la urna la que lleva señalada. Al salir entrega la nueva papeleta a la persona que controla la cadena de votación para repetir el proceso.

VVPAT (voter-verifiable paper audit trail) Sistema de votación electrónica que emite un comprobante en papel para permitir la realización, si fuera necesaria, de una verificación del proceso electoral.

VVSG (Voluntary Voting System Guidelines) Recomendaciones básicas para los sistemas de votación emitidas por la EAC (Election Assistance Commission).

1.Justificación, objetivos y estructura

"Siempre y cuando puedas empezar,
todo irá bien. Ya llegará el resultado"

Ernest Hemingway

"Divide las dificultades que examines
en tantas partes como sea posible,
para su mejor solución"

René Descartes

1.1. Introducción

Esta tesis pretende dar a conocer el porqué de las dificultades de hacer las cosas bien en el ámbito del voto electrónico, cuáles son las razones de las mismas y cómo podemos conseguir un uso correcto y sencillo de las tecnologías actuales en los diversos entornos de aplicación del voto electrónico en nuestra sociedad democrática. Para ello se analizan y comparan diversas soluciones propuestas con el objeto de conocer el grado de cumplimiento con los requisitos necesarios para llevarlos a cabo.

Se pretende conseguir que los procesos de votación electrónicos sean claros, sencillos y transparentes para lograr confianza en los mismos. Hasta el momento esa simplificación no se ha conseguido debido a los intereses encontrados entre los diversos actores que han intervenido en el panorama del voto electrónico. Desde mi punto de vista esos actores han sido:

- las empresas desarrolladoras de sistemas y soluciones poco proclives a auditorías abiertas;
- los Estados que han creado sus propios equipos y desarrollos;
- la comunidad científica que lleva décadas haciendo propuestas en su mayor parte teóricas;
- los ciudadanos que, con su uso y opiniones, han intervenido en su valoración.

Como fundamento de investigación para esta tesis doctoral, se parte de una serie de tecnologías que han sido utilizadas en muy diversos entornos y países. Analizaremos los casos más significativos, cómo han sido propuestos, cómo se han desarrollado y, si fuera el caso, cómo se han auditado. Nos interesa conocer los inconvenientes, las críticas, los análisis de los investigadores, las propuestas de mejora, todo con el afán de diseñar sistemas de votación electrónica que cumplan todos los requisitos esenciales para que sean vistos con la misma transparencia y seguridad que los comicios celebrados con procedimientos convencionales. Nos interesa dejar claro cuáles son los aspectos que habría que verificar antes de proponer un sistema y el procedimiento posterior que nos permita comprobar su transparencia y cumplimiento con los aspectos esenciales en cualquier proceso democrático. Aunque sea uno de los entornos que pueden digitalizarse, no podemos caer en la tentación de imponer la tecnología en el ámbito democrático a cualquier precio. Es decir, un análisis de las tecnologías utilizadas en el voto electrónico y su contexto.

A continuación se describirán los conceptos básicos relacionados con los sistemas de votación electrónica, revisaremos las distintas clases de sistemas que se han desarrollado bajo este término y la problemática concreta de seguridad que tiene su puesta en marcha y uso. Además, se recogen las soluciones más comunes a los problemas detectados así como aquellas dificultades que todavía no han sido superadas de forma clara debido a los complejos retos que son consustanciales a ellas. A partir de estas ideas, se clasificarán las posibles soluciones con objeto de poder conocer y comparar con facilidad el grado de cumplimiento de todos los aspectos de seguridad necesarios en el voto electrónico y en especial las soluciones con verificación de extremo a extremo (E2E) o, como propongo denominarla alternativamente, "verificación indirecta mediante recibo". Dicho de forma más concisa, una clasificación de los problemas y sus soluciones.

Es curioso observar cómo en pleno siglo XXI está resultando muy complejo desarrollar sistemas de votación electrónica que generen la confianza suficiente como para poder ser utilizados de forma habitual. Utilizamos las denominadas Tecnologías de la Información y de las Comunicaciones (TIC) en todo lo que nos rodea incluso en aquello de lo que depende nuestra propia vida (aviónica, sistemas de diagnóstico y tratamiento de enfermedades) o nuestro dinero (aplicaciones bancarias o de finanzas e inversión). Pero, en cambio, en lo que respecta a su utilización para la gestión de nuestros derechos democráticos no hemos conseguido diseñar los sistemas de forma que estos generen confianza. Nos hemos fiado de empresas que nos han vendido sus productos que han resultado poco seguros, también hemos confiado en los organismos de gestión electoral que nos hablaron de plena seguridad en los procesos electorales, incluso la comunidad científica ha publicado diversas soluciones apoyándose en complicados esquemas criptográficos sin obtener un uso y resultado tan sencillo y fiable como una votación convencional. En algunos países como Brasil, la India o Venezuela han optado por soluciones, que aun no siendo perfectas, facilitan el derecho al voto y un recuento rápido a pesar de las dificultades propias de su contexto poblacional y geográfico.

Sin duda una de las tareas más importantes de un gobierno democrático es la planificación y ejecución de las elecciones presidenciales o legislativas. Éstas no son las únicas en un contexto democrático pero sí las que precisan de unos requisitos más complejos de satisfacer. Pero las condiciones, limitaciones y especificaciones que se deben cumplir son extraordinariamente difíciles de satisfacer y dificultan en gran medida la introducción de los sistemas electrónicos que pueden estar sujetos a un gran número de ataques, manipulaciones e intrusiones por parte de enemigos internos o externos.

Por todo ello, y a lo largo de la historia reciente, hemos acumulado una colección de ejemplos de diseño pobre y defectuosa puesta en marcha de experiencias en buena parte del mundo, que han podido pasar más o menos desapercibidas. Desde manipulaciones en los contadores de las primeras máquinas con levas para contar votos, pasando por el nefasto procedimiento de lectura de las tarjetas perforadas, las insuficientes garantías de las urnas electrónicas, los procedimientos de coacción en cadena sobre los votantes o la poca transparencia y complicados procesos de observación externa en elecciones con voto electrónico, que nos han llevado a no poder contar con muchos ejemplos de éxito en la aplicación de las TIC en el voto electrónico, ya sea presencial o por Internet.

Un ejemplo claro y destacado fue lo ocurrido en las elecciones presidenciales de 2000 en los Estados Unidos en las que Bush ganó en el Colegio Electoral en Florida por un margen de 500 votos [7]. En esas elecciones el sistema de tarjetas perforadas no registró más de 50.000 votos por el denominado “efecto mariposa” [8] debido al cual el trozo de papel perforado no se desprendía y volvía a tapar el agujero imposibilitando su lectura. Y lo que es peor, este fallo era bien conocido por los funcionarios electorales mucho antes [9].

Como consecuencia de ello y para mejorar la velocidad y fiabilidad del recuento de votos, muchos estados consideraron conveniente utilizar equipos de votación electrónicos y a menudo tomaron apresuradamente decisiones que se convirtieron en nuevos problemas; algunos científicos aportaron pruebas de que el voto de esa manera complicaría o impediría por completo el proceso de verificación de las elecciones. Esto ha sido expuesto y defendido por expertos como Aviel Rubin [10], Rebecca Mercuri [11] y por informes de prestigiosas universidades como la de Stanford [12]. La controversia y el debate siguen incluso hoy en día.

En esta tesis, se analizan y comparan las soluciones más recientemente propuestas por la comunidad científica basadas en los últimos avances en los sistemas criptográficos de votación, proporcionando un tipo de sistema electoral que genera pruebas para poder verificar los resultados mediante recibos sin necesidad de auditar las máquinas, aspecto este que se ha demostrado muy complejo de diseñar y realizar.

1.2. Las razones del voto electrónico

Muchas son las preguntas sobre la necesidad real de utilizar la tecnología para resolver los procesos electorales. Sus defensores enfatizan las ventajas (como la

precisión y la rapidez) y minimizan los inconvenientes (como la falta de procesos de verificación sencillos que permitan comprobar que el proceso electrónico cumple con todos los requisitos necesarios). Alguno de estos aspectos son indiscutibles pero otros se dan por seguros incluso sin estudios básicos sobre el tema. Analicémoslos con más detalle.

Entre los aspectos positivos parecen destacar: precisión en la contabilidad de los votos, rapidez en el recuento, incremento de la accesibilidad para discapacitados o para personas con diversidades funcionales, ahorro de papel, flexibilidad, posibilidad de crear una infraestructura permanente para la opinión con voto, mejora de la eficiencia, etc. También se presentan como ventajas aspectos más discutibles como pueden ser el ahorro energético ya que las urnas tienen un determinado consumo en su fabricación y uso. Otro aspecto positivo es que su utilización parece ser más barata que el uso de la urna tradicional pero hay pocos estudios serios [13]. Por poner un ejemplo, en una de las últimas elecciones presidenciales con urnas electrónicas celebradas en Venezuela en diciembre de 2006 el coste estimado, por nuestra observación directa, fue de 200 millones de dólares. Por otro lado hay comparativas de costes en U.S.A. [14] entre las urnas basadas en sistemas con lectura óptica (optical scan systems) y urnas electrónicas con registro directo o DRE (direct recording electronic), pero la variación del precio de compra llega al 900% en función de las características del equipo y su configuración, destacando que en el caso de las DRE se factura el coste de la máquina y el del software de forma separada [15] [16]. También habría que incluir aquí el supuesto aumento de la participación, aspecto del que esta tesis no se va a ocupar [17] [18].

En cuanto a los inconvenientes también son variados y algunos no demostrados como ocurre en el párrafo anterior. Lo cierto es que en general la seguridad del proceso de votación está en entredicho y se concluye que la tecnología tiene demasiados riesgos. Como veremos en el capítulo siguiente, ha sido un error grave de ciertos desarrolladores e investigadores considerar que el nivel de seguridad de una votación electrónica es similar al requerido en una entidad financiera [19], cuando en realidad los requisitos de privacidad son absolutos y nadie puede analizar el proceso de votación desde dentro mientras se lleva a cabo, lo que complica de forma muy importante el diseño de soluciones con garantías de seguridad. Este tipo de requisitos nos obligan a utilizar diversas técnicas para poder verificar el voto, como el VVPAT (voter-verified paper audit trial, auditoría con comprobante en papel para verificación por el votante) [20] o técnicas de verificación de extremo a extremo (E2E). Hay claras dificultades en el diseño e implementación de la seguridad en estos equipos que deben tenerse en cuenta en todo momento para garantizar los requisitos de un proceso democrático [21] [22]. Otro aspecto negativo es el posible fraude que puede realizarse con algunos de estos dispositivos, si su diseño o su uso no es correcto. En este caso sí hay estudios rigurosos como los de Di Franco [23] que demuestran que con una pequeña manipulación en la copia maestra del software de votación es posible producir un fraude electoral a gran escala.

Sin haber resuelto completamente estos aspectos, la tendencia actual es el uso de Internet para la emisión del voto electrónico, lo que incrementa enormemente los riesgos en seguridad. Sin duda existe un elevado riesgo en seguridad por el mero uso de Internet (virus, troyanos, denegación de servicio distribuida, falta de control por las autoridades electorales de los equipos utilizados por los votantes, etc.) y por la baja transparencia del procedimiento incluyendo la posible pérdida del anonimato. Incluso el propio Vinton Cerf, considerado uno de los "padres" de Internet por su aportación al protocolo TCP/IP, considera que una de las debilidades de la Red es su baja seguridad. No es menos cierto que aparecen ventajas inherentes a la independencia del tiempo y del espacio en la emisión del voto, al probable incremento de la participación al evitar los desplazamientos, a la posible reducción del coste (si se tiene en cuenta en el diseño, fabricación y uso), etc. En cualquier caso, en esta tesis no se van a tratar los aspectos relacionados con el uso de las redes en el voto electrónico, o "Votación Telemática" según el profesor Carracedo [24].

1.3. Justificación

Es necesario precisar los requisitos del voto electrónico fiable y aumentar la confianza a través de las verificaciones claras y completas de este tipo de sistemas, aunque a pesar de todo podría ser considerado como insuficiente.

Si algo hemos aprendido a lo largo de estos años y mediante la experiencia acumulada, es que no es sencillo desarrollar con garantías procesos electorales apoyados en las tecnologías de la información. No es suficiente poner en marcha un equipo informático que cuente los votos emitidos. Es imprescindible verificar que lo hace respetando los requisitos necesarios en un proceso electoral democrático. Privacidad, inviolabilidad del sistema, integridad en el recuento y verificabilidad de todo el proceso, son aspectos necesarios para garantizar las bases democráticas de un proceso electoral. No podemos generar confianza en el electorado si no cumplimos escrupulosamente con todos estos requisitos.

A pesar de las soluciones que de forma continua aparecen, ya sea a nivel académico y formuladas como propuestas para su debate y valoración, o bien a nivel comercial como sistemas cerrados que dicen cumplir con los requisitos necesarios, es preciso realizar un esfuerzo de investigación con objeto de dejar claro cuáles son las debilidades y las fortalezas de cada una de ellas.

1.4. Objetivos

El objetivo principal de esta tesis es detectar, analizar, valorar y comparar las últimas propuestas en el voto electrónico PRESENCIAL, basadas en verificaciones de extremo a extremo (E2E), permitiendo su clasificación atendiendo a niveles de cumplimiento de los criterios básicos de un proceso de votación democrática. Para ello en el siguiente capítulo se fijarán estos criterios y posteriormente, en el capítulo 4, se analizarán una a una las soluciones propuestas y se valorarán para determinar

el nivel de cumplimiento de los mismos, estableciendo una clasificación comparada.

De forma más detallada y clara los objetivos de esta tesis son:

- En primer lugar, encontrar y distinguir las propuestas académicas que existen sobre voto electrónico presencial con posibilidad de verificación de tipo E2E. Posteriormente, contrastar y filtrar con criterios de calidad la información publicada en los diversos medios y la obtenida de las experiencias realizadas.
- Después, analizar la información que de cada solución exista y clasificarla en función de los requisitos necesarios en los procesos de votación democrática, valorando su grado de cumplimiento, las fortalezas, las debilidades y las vulnerabilidades conocidas o probables.
- Además, se elaborará una comparación entre todas ellas basada en la información disponible con objeto de establecer un criterio más de clasificación.
- Por último, se desarrollará una evaluación crítica de cada una de las propuestas, con objeto de obtener una idea clara del grado de cumplimiento en función de los criterios señalados. Para ello se confeccionará una tabla que permita la comparación entre todas las soluciones.

1.5. Metodología

En primer lugar se recopilará la información disponible de las soluciones propuestas y de las experiencias de uso con objeto de poder valorarlas con los criterios de integridad, privacidad, fiabilidad, usabilidad, verificabilidad y sencillez. Posteriormente se analizarán de forma individual y comparada todas estas soluciones, extrayendo y criticando cada uno de los aspectos esenciales que configuran un proceso de votación electrónica que ha de cumplir con los criterios señalados. Para ello se utilizará con una visión crítica toda la información disponible, ya sea generada por los autores, por los expertos o por los informes extraídos de las experiencias de uso real.

1.6. Estructura de la tesis

Comenzaré con una revisión de los requisitos funcionales de las votaciones apoyadas en las TIC y de una visión general de los conceptos técnicos básicos necesarios en materia de seguridad en las votaciones electrónicas. Después repasaré la panorámica de sistemas y experiencias del voto electrónico a nivel mundial. Más tarde elaboraré unos criterios básicos y claros que nos permitan la evaluación, clasificación y comparación de la excelencia de los sistemas de voto electrónico. Por razones puramente prácticas me limitaré al voto electrónico

presencial, ya que el remoto o telemático plantea problemas de otra índole. Por último, presentaré las conclusiones.

El recorrido global por los capítulos que constituyen esta tesis es:

- En el capítulo 2 se presentan con detalle los problemas del voto electrónico y la evolución histórica de las soluciones propuestas.
- En el capítulo 3 se presenta el estado del arte actual.
- En el capítulo 4 se describen, analizan y comparan las propuestas más actuales, dentro de las soluciones de tipo E2E.
- En el capítulo 5 se establecen las aportaciones y conclusiones de esta tesis, así como las propuestas de trabajos futuros.

2

2.Exposición del problema y evolución de las soluciones

Доверяй, но проверяй
Confía, pero verifica

(Proverbio ruso)

2.1. Definición de voto electrónico

El Consejo de Europa [25] define "voto electrónico" como aquel donde al menos el voto es emitido por medios electrónicos. Esta definición no es muy clara si queremos realizar un estudio en profundidad y necesitaría ser matizada, tanto en sus aspectos tecnológicos como sociales [26].

2.2. Tipos de votación electrónica

Existe una gran diversidad de formas de votar y de sistemas involucrados en los procesos de voto electrónico que se han clasificado de diferentes maneras según el punto de vista elegido por los autores de esas clasificaciones. Para facilitar su comprensión y flexibilidad, partiremos de la más sencilla que es la que se produce al dividir los procesos de votación en presenciales y no presenciales.

Así, hablaremos de proceso de votación presencial cuando, previa identificación del votante, se le autoriza a votar con ayuda de una máquina dispuesta en un lugar específico (colegio electoral) y que mediante lectura óptica (OCR) o registro electrónico (DRE) deposita y almacena electrónicamente el voto. En este caso el proceso de identificación es independiente y no debe de existir la posibilidad de relacionarlo con el voto depositado y además toda la información necesaria está "in situ". Para ello se utilizan equipos específicos.

Por el contrario cuando el voto es ejercido no presencialmente, es decir, de forma remota, utilizando medios telemáticos (votación telemática) o más concretamente Internet, el sistema lo hace todo (identificar y enviar el voto) y

probablemente con independencia del dispositivo (ordenador personal o equipamiento equivalente). Por tanto, en este caso no se utiliza un equipo específico para votar.

Clasificaciones más pormenorizadas permitirían ver con más detalle los sistemas utilizados y su evolución. Sistemas tradicionales: papeletas, tarjetas perforadas, máquinas de palancas o levas. Sistemas de voto electrónico convencionales (genéricamente urnas electrónicas), como urnas con OCR (lectores ópticos de caracteres) o DRE (en general con pantalla táctil y almacenamiento de datos en dispositivos basados en semiconductores). Voto remoto o telemático, ya sea en quiosco electoral ubicado en cualquier parte, en quiosco electoral ubicado en colegio electoral o sobre cualquier dispositivo con conexión a Internet y desde cualquier parte (voto remoto puro).

Las estadísticas de uso son muy variadas en función del país y el tipo de urna, pero las urnas electrónicas más utilizadas en U.S.A. desde el 2004 son las ópticas seguidas por las DRE. En cambio el voto telemático puro se ha utilizado en muy pocos países y menos de forma vinculante como ha sido el caso de Estonia desde el 2005 y en Noruega en 2011 y 2013.

Si nos centramos en los dispositivos electrónicos que podemos utilizar en el voto electrónico, podemos clasificarlos en función de su uso controlado o no controlado.

En el primer caso podemos tener:

- Dispositivos de voto electrónico independientes o autónomos (stand-alone).
- Dispositivos de voto electrónico conectados a red (networked).

Y en el segundo:

- Dispositivos para voto electrónico remoto o telemático (PCs, móviles, PDAs), también conectados a red.

Incluso podemos considerar el caso de dispositivos que puedan utilizarse en ambos ambientes, controlados y no controlados:

- Quioscos para voto electrónico conectados a red.

En función de los aspectos automatizados resulta útil establecer una clasificación de los sistemas de votación en tres niveles [27] , tal como se indica a continuación.

En un primer nivel de automatización del proceso electoral que denominaremos básico se utilizan dispositivos electrónicos, herramientas informáticas y medios telemáticos para agilizar los procesos administrativos que tienen que ver con la emisión del voto, como son: el registro de votantes, la generación y publicación del censo electoral, la impresión de todas las actas necesarias y la transmisión de resultados de votación (independientemente de que se utilicen o no otros medios no electrónicos) Este primer nivel puede ser adecuado para aquellos países en los que han funcionado adecuadamente durante tiempo y no se han observado dificultades específicas. Concretamente es el caso de España en

el entorno de las elecciones políticas en todos sus niveles y que se ha denominado "mesas administradas electrónicamente" [28].

En el siguiente nivel, denominado intermedio, se introduce la automatización de los procesos de emisión y recuento del voto. Las urnas convencionales en las que se introducen los votos en papel se sustituyen por sistemas informáticos, denominados "máquinas o equipos de votación", que pueden sustanciarse en DRE (direct-recording electronic machine), que capturan y almacenan el voto de forma electrónica y permiten realizar automáticamente el recuento al terminar la votación o en sistemas que permiten la lectura óptica de los votos (OCR) y su procesamiento posterior. Como podremos comprender a lo largo de esta tesis, estos equipos tienen defensores y detractores y cada uno pone de relieve sus ventajas e inconvenientes. Los ejemplos más importantes de uso están en la India, Brasil, Venezuela y en algunos estados de los EE.UU. [29] [30] [31] , donde se han implantado sistemas de voto electrónico que encajan en esta clasificación.

Cuando al anterior nivel se le añade el uso de redes telemáticas obtenemos el nivel avanzado de automatización en los procesos electorales. En este caso los votos se depositan en una urna remota sin control del votante. A este caso lo denominamos voto telemático (telematic vote) también conocido como voto remoto (iVoting) y con cierta frecuencia puede crear confusión con el anterior [24]. En este nivel está incluido el proceso electoral completo, desde la identificación de cada votante hasta la publicación de los resultados.

2.3. Características ideales del voto electrónico

Es necesario garantizar una serie de aspectos en el voto electrónico para conseguir que cumpla con los requisitos que imponen los sistemas democráticos, lo que hace que las posibles soluciones sean cuando menos complejas. Estos requisitos han sido descritos por diversos autores y desde puntos de vista muy variados: desde los considerados pioneros como el de Rebecca Mercuri [32], los que abordan las propuestas desde un punto de vista de la ingeniería [33], o de los requisitos funcionales [34], del diseño y la implementación [35], de la evaluación [36] o sencillamente de la gestión [37].

En general, y aglutinando los requisitos necesarios y los deseables, son los siguientes:

1. Autenticación: que sólo puedan votar los que estén legitimados para ello y todos los legitimados puedan hacerlo.
2. Unicidad del voto (democrático): que sólo se pueda votar una vez y no se pueda modificar este voto una vez emitido, aunque en algunos casos pueda votarse varias veces y sólo se contabilice la última.
3. Anonimato: que no se pueda relacionar el votante con el voto emitido.
4. Secreto del voto: que no se pueda relacionar el voto con el votante.

5. Imposibilidad de coacción: el votante no puede en ningún caso ser capaz de demostrar qué voto emitió, impidiendo la compra masiva de votos y la presión (coacción) sobre los votantes.

6. Precisión: el sistema tiene que poder registrar los votos correctamente y con seguridad.

7. Verificación (trazabilidad): cada votante podrá obtener una prueba (recibo) del sistema de votación que le garantice que su voto ha sido incluido en el escrutinio final sin alteraciones. Existen diversos niveles de verificación como veremos más adelante.

8. Imparcialidad: todos los votos deberán permanecer en secreto hasta que finalice el periodo de votación. De esta forma se evita que los resultados parciales afecten a la decisión de los votantes que no han votado.

9. Auditabilidad: que existan procedimientos para poder verificar que los sistemas involucrados han funcionado correctamente, sin sufrir manipulaciones o errores.

10. Confiabilidad: los sistemas utilizados deben trabajar de modo seguro siempre, sin que se produzcan pérdida, inclusión o modificación de votos incluso en casos extremos.

11. Flexibilidad: los equipos involucrados en la voto electrónico deben ser flexibles con los formatos utilizados (idiomas, posibles elecciones a distintos órganos, diversos tipos de papeletas de votación) y ser compatibles con todo tipo de plataformas y tecnologías.

12. Accesibilidad: que permita ejercer el voto a personas con diversidad funcional en distintos grados.

13. Facilidad de uso (usabilidad): los votantes tienen que ser capaces de votar con unos requisitos mínimos en formación y entrenamiento. El diseño de la aplicación tiene que ser sencillo, claro y compatible con la tradición electoral y por tanto que se parezca todo lo posible a una urna convencional en su aspecto y uso.

14. Eficiencia en el coste: los sistemas tienen que ser asequibles y reutilizables fácilmente.

15. Certificables: los sistemas deben poder comprobarse por parte de las autoridades electorales, de forma que se pueda validar el cumplimiento con los criterios establecidos.

16. Invulnerable, impidiendo la manipulación a todos los niveles y en todo momento.

17. Abierto, de forma que las autoridades electorales y, si es el caso, el ciudadano en general puedan obtener detalles de su funcionamiento (hardware y software).

18. Barato, de forma que sea competitivo con el voto tradicional.

Sin duda que el cumplimiento en mayor o menor grado está en función de los diversos puntos de vista de los elementos involucrados: administración, ciudadanos (electores), empresas y la academia. De esta forma la administración en general opina que los procesos electorales son complejos, costosos y en algunos casos poco

eficientes y problemáticos, por lo que intentan utilizar las TIC para su simplificación, mejora y abaratamiento. Los ciudadanos observan que los métodos utilizados son arcaicos y en algún caso poco fiables (papeletas perforadas en el estado de Florida en noviembre del 2000, voto por correo en algunos países, etc.) pero no están seguros de que los nuevos métodos tecnológicos cumplan los requisitos imprescindibles. Las empresas ven una oportunidad de negocio al ofrecer máquinas que cumplen con su cometido y muy probablemente bien desarrolladas, pero con escaso control por parte del contratante e intentando mantener la solución como una "caja negra" y con pocas o nulas posibilidades de verificación externa y abierta. La academia ve todo esto como un reto científico y tecnológico e intenta desarrollar soluciones que minimicen los problemas y garanticen el cumplimiento de los requisitos necesarios, al menos de forma teórica.

2.4. Requisitos necesarios del voto electrónico

El uso de la tecnología digital para la emisión del voto, almacenamiento y recuento, abre la posibilidad de conseguir una serie de supuestas ventajas y aportar soluciones a una de las actividades democráticas más rigurosas en cuanto a requisitos que se deben satisfacer. Es por ello que engañosamente se ha considerado que utilizar las TIC en el entorno de los procesos electorales no era más que otro reto en la aplicación de las mismas. La experiencia acumulada hasta ahora nos enseña que no es así, ya que debemos satisfacer simultáneamente y con garantías los siguientes requisitos:

- Los sistemas y equipos utilizados deben estar protegidos contra cualquier tipo de ataque y manipulación, antes, durante y después de la emisión del voto. La disponibilidad de los sistemas ha de estar garantizada. Se denomina a este requisito: INVIOLABILIDAD o ROBUSTEZ.
- Uno de los aspectos más complejos que han de cumplir los sistemas de voto es la PRIVACIDAD. Esto a su vez tiene dos apartados: la anonimia y mantener el voto secreto.
    - Los votantes presentes en el censo electoral han de ser autorizados para utilizar el sistema de forma privada y para emitir una sola vez el voto. En el equipo no ha de quedar ningún registro de la identidad del votante que pueda relacionar el voto emitido con la identidad del mismo, ni mecanismo para deducirla directa o indirectamente. Se denomina a este requisito: ANONIMIA.
    - El VOTO SECRETO consiste en que cada voto que ha sido emitido se mantenga en secreto hasta el momento del recuento.

  En realidad estos dos apartados son dos caras de la misma moneda y tratan de evitar que un observador externo pueda relacionar al votante con su voto y el contenido del mismo con el votante. La anonimia se relaciona con el votante porque una vez que deposita el voto en la máquina el propio votante desconoce cuál es, y con el secreto del voto porque no debería de poder relacionarse el contenido del voto con el votante en ningún momento.

Otros aspectos necesarios si el sistema emite recibo en la votación son: el recibo libre de coacción y el sistema resistente a las coacciones.

- Recibo libre de coacción. Este requisito tiene que impedir al votante demostrar qué o a quién ha votado: el recibo debe demostrar que se ha votado pero no qué o a quién, de forma similar al procedimiento de marcar un determinado dedo del votante con tinta indeleble. Este requisito debería impedir la venta de votos.
- Sistema resistente a la coacción. En este caso es el sistema el que debe evitar que se pueda ejercer coacción directa o indirecta sobre el votante, aún con la ayuda de éste.

- Es necesario garantizar que el resultado de las elecciones no pueda ser alterado o manipulado de ninguna forma. La protección de los votos digitales emitidos ha de ser total. Nadie puede llegar hasta ellos salvo en el momento del recuento, impidiendo su manipulación, eliminación o la adición de votos. Se denomina a este requisito: INTEGRIDAD. Los procesos electorales están constituidos por tres pasos: depositar el voto, registrarlo y realizar el recuento.
  - En la fase de depósito es imprescindible asegurar que se realiza de tal forma que coincida con la intención del votante. Esta condición tiene que ver más con la usabilidad del sistema que con las condiciones de seguridad.
  - En el paso de registro tenemos que garantizar que el voto es almacenado tal y como ha sido depositado por el votante.
  - En el último paso es necesario asegurarnos que el recuento se realiza exclusivamente con los votos que han sido registrados en el paso anterior y de forma correcta. El recuento de votos ha de ser rápido y preciso, sin posibilidad de manipulación ya sea por los propios responsables del mismo o por terceros.
- La posibilidad de verificar los votos emitidos, tanto por el votante con respecto a su voto como de forma general por las autoridades electorales, tiene que ser viable. El recuento tiene que tener carácter público. Se denomina a este requisito: VERIFICABILIDAD. Este requisito no siempre se ha podido cumplir y tiene todo su sentido y desarrollo en los sistemas denominados de verificación extremo a extremo o *end-to-end* (E2E). Puede tener varios aspectos:
  - Verificabilidad individual. Con este requisito permitimos al votante comprobar que su elección al votar ha sido correctamente registrada y codificada en su recibo y puede utilizar éste para verificarlo.
  - Verificabilidad pública. Con esta característica cualquiera podría verificar que todos los recibos mostrados en el tablón postelectoral han sido correctamente descifrados y contabilizados.
  - Verificabilidad extremo a extremo. En este caso garantizamos que todos los pasos de una votación pueden ser

comprobados y que el resultado de la votación coincide con el recuento de todos los votos según fueron emitidos. Este tipo de verificación puede ser pública o individual o una combinación de ambas.

La verificabilidad es un requisito esencial ya que la emisión del voto electrónico supone una falta de transparencia para el votante que debe ser compensada con algún mecanismo que permita la trazabilidad sobre su voto, sin que ello dé ocasión a la posibilidad de llevar a cabo algún tipo de coacción sobre el mismo.

A lo largo de los últimos veinte años de uso de la votación electrónica, se ha venido a demostrar que no es sencillo cumplir con todos estos requisitos, a los que se pueden añadir otros aspectos deseables. Existen funcionalidades no imprescindibles pero que, sin duda, mejoran el proceso de votación, como las siguientes:

- USABILIDAD. Esta se consigue con un buen diseño del proceso en sí y de la interface con el usuario, consiguiendo que sea sencillo, intuitivo, claro y fácil de utilizar.
- ADAPTABILIDAD en tiempo al votante, permitiendo que los votantes menos instruidos o con problemas de aprendizaje puedan votar utilizando más tiempo del habitual.
- ACCESIBILIDAD al sistema de votación, facilitando el voto sin ayuda externa a personas con diversidades funcionales, incluso con ceguera.
- VERSATILIDAD del sistema de votación, de forma que pueda utilizarse en diversos tipos de votaciones y condiciones.

2.5. El problema de la seguridad

Es necesario fijar con claridad las dificultades específicas que tiene la implementación de una solución tecnológica en un proceso genérico de votación, con el fin de respetar las reglas básicas que permitan generar confianza en el electorado.

Ha sido un error grave de algunos desarrolladores e investigadores considerar que el nivel de secreto de una votación electrónica es similar al requerido en una entidad financiera, cuando en ésta la operación puede ser conocida por terceros autorizados y en cambio en el voto electrónico el anonimato es parte esencial del mismo, con lo que NADIE puede tener información sobre quien lo emitió [38]. Esta restricción nos obliga a utilizar diversas técnicas para poder verificar que nuestro voto ha sido correctamente contabilizado sin desvelar el votante. Por ejemplo, los sistemas basados en el VVPAT complican y ralentizan el uso de las máquinas utilizadas para el voto electrónico ya que tienen que imprimir el voto para posteriormente ser depositado en la urna y a pesar de todo hay claras limitaciones en la seguridad de estos equipos si no se toman las medidas oportunas.

No obstante, las limitaciones en la seguridad no deben desanimarnos pues hay suficiente conocimiento para diseñar procesos de votación electrónica

razonablemente seguros y fiables. Está claro que todo se basa en generar CONFIANZA en el electorado y esto no se consigue de un día para otro.

Si bien es cierto que la criptografía puede ser una excelente aliada para resolver problemas complejos, no es menos cierto que la verificación de un proceso electoral es aún más difícil, como podremos descubrir en esta tesis. En este sentido, vamos a intentar demostrar que votar es un problema único y que la criptografía bien aplicada nos puede ayudar a resolverlo, siendo una de las posibles soluciones utilizar métodos de auditoría abierta, evitando el uso de tecnologías cerradas y propietarias tanto de empresas como de estados.

También se cometió el error de considerar que la seguridad necesaria en un proceso electoral no era más compleja que la necesaria para controlar la aviónica de un aeroplano o la seguridad bancaria [39]. Y no son comparables puesto que el secreto del voto, tanto de lo que se vota como de quién lo realiza, está en conflicto con los procesos de auditoría necesarios para generar confianza y es aquí donde aparece como necesaria la criptografía [38].

Ha sido habitual que los procesos electorales apoyados en tecnología en mayor o menor grado carecieran de transparencia en parte del proceso. Generalmente el fabricante de la solución electrónica para la votación imponía una caja negra entre el depósito del voto y el recuento. Han sido numerosos y diversos los ejemplos de un uso incorrecto de este tipo de soluciones [40] [41] que han contribuido a generar dudas y no pocos detractores [11] [42]. En una palabra, en vez de generar confianza, han incrementado las dudas.

¿Por qué es tan complejo el voto electrónico seguro y verificable? Son varios los aspectos que confieren al voto electrónico una dificultad única para poder ser resuelto con plenas garantías democráticas [43]. Estos pueden clasificarse en: intereses creados, tipo de adversarios y dificultad para detectar y recuperar fallos.

El interés en manipular unos resultados electorales son evidentes por las ventajas sociales, económicas o políticas que se podrían obtener [9].

Los tipos de adversarios que podrían atacar un proceso electoral son muy diversos, desde el propio votante, las autoridades electorales, los candidatos o cualquier tipo de colusión entre ellos. Es decir, no están delimitados ni aislados como puede ocurrir en otros casos como en la banca o en la aviación donde este tipo de riesgos están más acotados y estudiados, con auditorías de terceros específicamente diseñadas para detectarlos. Esto es así, debido a que en el caso de las votaciones nadie debería de poder observar el proceso electoral desde dentro del sistema lo que podría complicar enormemente la detección de manipulaciones, ataques o errores.

En la votación electrónica es necesario repetir el proceso para recuperar un error una vez que el voto ha sido emitido o bien cuando se verifica que el recuento ha sido incorrecto. En aviación existen las cajas negras que nos indican mediante registro de todos los datos donde se han producidos los errores o fallos con objeto de corregirlos y que no vuelvan a ocurrir. Al igual que en la banca se hace mediante recibos. En el voto electrónico no es posible este tipo de control por lo que la detección de los errores se efectúa tarde o nunca. Además, si lo detectamos, lo único

que podemos hacer es repetir el proceso de votación desde el comienzo o conformarnos con el resultado aunque no respete la esencia democrática [44].

2.5.1. El problema de la seguridad en los procesos electorales clásicos

En general y en un proceso electoral clásico con votación presencial y en urna, se consigue el anonimato en el mismo momento en que uno deja caer la papeleta de voto, ya que se separa sin posibilidad de vuelta atrás la identidad del votante y su voto. Posteriormente, siempre y cuando el proceso esté diseñado con suficientes garantías, la custodia de los votos y el recuento público generan confianza en los resultados. De esta forma cumplimos con los requisitos básicos de un proceso de votación democrático. La transparencia del sistema es tal que cualquier elector puede auditar el proceso de principio a fin permaneciendo en el colegio electoral y observando la emisión de todos los votos en las urnas ubicadas en ese centro electoral y posteriormente presenciado el recuento, la elaboración de las actas de resultados y la publicación de todas y cada una de las actas de todos los colegios electorales a nivel nacional e incluso si fuera el caso, internacional. Es decir una total transparencia. Adicionalmente el sistema se refuerza con un protocolo de cadena de custodia de todos los resultados parciales con varios canales de verificación que en paralelo comprueban que ningún resultado pueda ser modificado en ninguna etapa del proceso. El hecho de que todo sea público y pueda ser verificado en todos los niveles por representantes de los elegibles (interventores) en la votación confiere al sistema una gran robustez.

Además, este tipo de elecciones tienen que ser capaces de permitir que muchos miles de votantes puedan ejercer su derecho u obligación de votar en un período de tiempo relativamente corto y que el recuento sea realizado en un espacio de tiempo lo más reducido posible para evitar retrasos innecesarios y suspicacias.

De aquí las cuatro condiciones básicas de un proceso electoral: anonimato, precisión y rapidez en el recuento y fiabilidad [45].

Al mismo tiempo, y en la mayor parte de los procesos electorales, existen determinados canales de participación en los que no está tan claro que se respeten todos los requisitos necesarios de un modelo democrático de participación. Es el caso del voto por correo o, en el caso de España, de la participación a través de embajadas y consulados que permiten la votación del denominado C.E.R.A. (censo electoral de los residentes ausentes) regulado por la Ley Orgánica del Régimen Electoral General, LOREG 5/1985 de 19 de junio. En ambos casos no es posible auditar de forma transparente el procedimiento de custodia de los votos e incluso la identificación del votante, con lo cual no puede calificarse de totalmente confiable. En este caso prevalece la necesidad de cumplir con el artículo 23 de la Constitución Española garantizando la posibilidad de participar, antes que la seguridad del proceso.

2.5.2. El problema de la seguridad en los procesos electorales electrónicos

En el momento en que se han introducido las tecnologías de la información y las comunicaciones en los procesos electorales, la transparencia clásica se pierde. No podemos visualizar de forma abierta y pública el flujo de información binaria que entra en los sistemas digitales (equipos de votación, equipos de transmisión, redes…) y por ello no podemos estar seguros *a priori* de que se cumplen los requisitos básicos en una democracia. Existen infinidad de ejemplos en los que se ha confiado en las empresas que desarrollan estos sistemas y soluciones, que han defraudado de una forma clara [46] [47].

Estas tecnologías han de ser capaces de cumplir con los requisitos de preservar el anonimato y contabilizar el voto de forma correcta bajo cualquier circunstancia, pero además, como el proceso en sí no es transparente, deben proveer de los mecanismos que permitan auditar todo el proceso en general y cada voto en particular.

Además, si esto no fuera suficiente, aparece la nueva condición de que la auditoría que puede ejercer el ciudadano esté exenta de la posibilidad de coacción.

De la misma forma que en los procesos de voto clásico, es necesario establecer una cadena de custodia de los equipos que se van a utilizar para ejercer el voto y posterior recuento, de manera que se evite cualquier tipo de manipulación no autorizada.

En cuanto introduzcamos un dispositivo electrónico en un proceso de votación, todos los elementos que lo componen deben cumplir al menos con los requisitos de mantener el anonimato y la fiabilidad en el recuento [48]. Para ello todos los elementos utilizados en el dispositivo, desde la propia arquitectura del procesador y sus memorias, el firmware, el sistema operativo, las aplicaciones utilizadas para el registro del voto y el recuento, deben cumplir en todo momento con el objetivo de mantener la anonimia y la precisión en el conteo de los votos, así como impedir cualquier tipo de influencia externa sobre el mismo por minúscula que sea [23]. Por si fuera poco, estas condiciones se han de poder verificar antes, durante y después de la votación. La verificación de todos estos requisitos lo podríamos realizar mediante una auditoría que compruebe todos y cada uno de los elementos implicados durante todo el tiempo, algo que no solamente puede parecer complejo sino que se ha revelado impracticable. Son las auditorías que denominaremos clásicas o directas y hay muchos ejemplos a lo largo de los últimos años de dificultades en su realización [5], de fraudes [30], fallos [21], riesgos en los precintos [49], vulnerabilidades en el software [40] [50] [51] y en el hardware [52] [29].

2.6. Necesidad de la auditoría

El primer paso de los especialistas en seguridad de la información fue recrear digitalmente los procesos físicos necesarios en una votación, lo que les permitió descubrir el nuevo paradigma de la votación, la necesidad de conjugar el secreto del voto y de la auditoría, es decir "la revisión sistemática de una actividad para evaluar el cumplimiento de los criterios objetivos a que aquellas deben someterse" [53].

El recuento de votos emitidos públicamente es sencillo al no necesitar mecanismos para preservar el anonimato, tan sencillo como sumar con garantías de integridad. De la misma forma hay que hacerlo en una votación anónima sin posibilidad de unir el voto al votante, lo que puede ser aprovechado para manipular los votos. De ahí la necesaria auditoría que garantice la correcta contabilidad del proceso y permita al votante comprobar que su voto ha sido tenido en cuenta tal y como lo emitió. Dicho de forma general: que cada uno pueda verificar su propio voto y que cualquiera puede comprobar de forma global todo el recuento. Esto se define como la posibilidad de verificar de principio a fin el proceso o verificación de extremo a extremo. Para ello es necesario algún tipo de recibo que nos permita la comprobación y que será entregado en el momento de la votación con el fin de utilizarlo posteriormente para confirmar el voto emitido y su correspondiente contabilización. Pero también es necesario que ese comprobante no pueda ser utilizado por un tercero para verificar cuál ha sido nuestro voto y ejercer algún tipo de coacción sobre nosotros. Por último se debe proteger al sistema frente a falsas acusaciones. A poco que pensemos sobre ello, descubriremos la dificultad de su diseño y puesta en marcha.

Si cada votante utiliza su comprobante y cualquiera puede verificar la correcta contabilidad del proceso, habremos conseguido un proceso electoral confiable al disponer de una auditoría abierta (*open audit voting*).

Para conseguir esto es necesario cifrar el voto en el momento de su emisión y separarlo permanentemente de quien lo emitió para inmediatamente después emitir el comprobante que puede ser utilizado para verificar el registro y posterior recuento sin descubrir el sentido del mismo. Todo un reto. Para ello se pueden utilizar diversas técnicas de cifrado, desde las basadas en números aleatorios como en el caso del Bingo Voting que estudiaremos más adelante, como combinando una clave pública y una o varias claves privadas o mediante cifrado basado en homomorfismos o *mixnets.* Es en este último tipo de soluciones donde se encuentran la mayor parte de las propuestas viables y sobre todo auditables, como las desarrolladas por Adida [54], Benaloh [55], Neff [56], Cramer [57], Schoenmakers [58], Chaum [59], Rivest [60], Ryan [61], Schneier [62] y Benaloh [55] entre otros. Además existen desarrollos disponibles como los de Scantegrity [63] y SCV [64].

A pesar de que somos muchos los que creemos en la viabilidad del voto electrónico, si no conseguimos desarrollarlo con auditorías abiertas, el panorama seguirá siendo tan sombrío como ha quedado demostrado hasta ahora en buena parte

de las experiencias mundiales que estudiaremos a continuación. Ojalá que en breve espacio de tiempo consigamos que el uso de las tecnologías en los procesos electorales sea tan habitual como la criptografía de clave pública, en la que parte del secreto es conocido por todos [24].

La criptografía o cifrado es el núcleo central de la seguridad en un sistema de voto electrónico como se ha demostrado en las soluciones desarrolladas por los expertos tanto en voto presencial como telemático. Una de las primeras propuestas de cifrado para la protección de la identidad del votante la propuso David Chaum en 1983 [65] y posteriormente le han seguido un sinnúmero de ellas generadas, en su mayor parte, en el ámbito académico.

Los métodos clásicos utilizados para garantizar la integridad electoral, tienden a centrarse en los mecanismos de verificación que se habilitan en cada paso de la cadena de votación, desde la intención del votante hasta el recuento final, y los diseñadores saben desde hace tiempo que tal enfoque puede pasar por alto algunas vulnerabilidades y sobreproteger otros aspectos, dificultando su diseño, puesta en marcha y auditoría [5] [66] [67] [68] [69]. Los procesos de votación son un ejemplo de sistemas en los que se pueden aplicar los criterios de diseño "End to End" y de esta forma se simplificarían los mismos en sus pasos intermedios, poniendo todo el esfuerzo de gestión y comprobación de la integridad de la información en los extremos del sistema de votación electrónica [70]. De esta forma no es necesario diseñar los pasos intermedios del transporte de la información con un control de la seguridad muy exigente. Esta alternativa ha sido utilizada en Internet, con el fin de proteger la integridad de toda la cadena de transporte de la información [71].

Un primer intento de aplicar la tecnología en los procesos electorales se sustanció en el uso de la lectura óptica de las papeletas de votación mediante urnas con OCR. Incluso en nuestro país se diseñó y utilizó una de estas urnas desarrollada con el apoyo del Gobierno Vasco [72]. Las experiencias tuvieron sus inconvenientes, como el uso de un papel especial, la incertidumbre de la opción marcada y problemas con la incidencia de la iluminación sobre el lector. El fracaso de los sistemas de votación de escaneo óptico en cuanto al cumplimiento de los razonables estándares de usabilidad se puso de relieve en el año 2002 [73].

La gestión de la integridad de una elección a menudo implica múltiples pasos. Se espera que los votantes rellenen su voto según lo deseado y lo hagan de forma correcta para posteriormente hacer una auditoría de las urnas recontando manualmente los votos y comprobar que coinciden con el recuento basado en el reconocimiento óptico de las marcas. Posteriormente se publican los recuentos de cada urna y se utilizan éstos para permitir la verificación pública. La pregunta es, ¿cuál es la precisión en el resultado de la elección, tal y como se refleja en el escrutinio oficial, con respecto a la intención real de los votantes que participaron en las elecciones? Aquí aparecen una serie de imprecisiones entre la verdadera intención del votante y la marca depositada sobre la papeleta especial para este tipo de urnas ópticas, así como determinar qué es una marca física aceptable y legalmente vinculante. Para cada sistema de lectura de papeletas los proveedores

deberían documentar la clase de marcas que van a ser contabilizadas de forma fiable y las que no lo van a ser. Además en cualquier sistema real, también podrían aparecer marcas marginales, es decir que no coincidan plenamente con el espacio reservadas a las mismas, que podrían ser contadas en algunas circunstancias y en otras no.

El siguiente paso del voto electrónico se desarrolló a partir de 1996 sobre equipos denominados DRE (Direct Recording Electronic) que en la mayor parte de los casos disponían de una pantalla táctil pero sólo quedaba constancia del voto en la misma. Este tipo de equipos son los utilizados en la India y Brasil y están siendo muy atacados por sus posibles vulnerabilidades y su compleja auditoría [40] [29]. Todos los sistemas de votación están sujetos a las limitaciones y los riesgos de la tecnología informática. Esto incluye la dificultad de verificar todos los aspectos necesarios y en todos los equipos, antes, durante y después del proceso electoral, con el fin de detectar la presencia de hardware o software que podría ser utilizado, en forma deliberada o inadvertidamente, para alterar los resultados de las elecciones [74].

En principio todos los sistemas de votación necesitan de un cuidadoso diseño para que puedan funcionar de forma fiable en entornos que no siempre van a ser ideales. Si el proceso electoral se desarrollara en un entorno ideal sólo habría que desarrollar un protocolo *P* que a través de un canal seguro identificara a los *n* votantes y les diera la oportunidad de emitir su voto V_i (siendo *i* un valor de 1 a *n*). Posteriormente y finalizada la votación, se realizaría el recuento con una función definida $f(V_1..Vn)$ y se publicarían los resultados. El problema principal es que hay que evitar a toda costa que los observadores externos puedan conocer el autor de cada voto V_i. Sería fácil crear algún tipo de ataque o buscar vulnerabilidades para atacar el protocolo *P* y conseguir que la función de recuento no funcionara correctamente. Estaríamos introduciendo una variante en el protocolo, que podríamos definir como *Q*, que daría lugar a una colección de votos Q_i que diferiría del original en mayor o menor grado. En este último caso estaríamos hablando de una votación en el mundo real y la diferencia entre la colección de votos V_i y Q_i no debería existir. Por supuesto pueden existir otros tipos de ataques que puedan poner en jaque la propia función *f()* de recuento (falta de fiabilidad) o la posibilidad de convertir el canal seguro de votación en inseguro (falta de anonimato).

2.6.1. La primera solución (VVPAT)

El primer tipo de auditoría que apareció en los equipos de votación electrónica fue el denominado VVPAT (voter-verified paper audit trail) diseñado en el 2002 por la Dra. Mercuri [32] [75] y por ello también conocido como método Mercuri; en esencia es una vuelta al uso del papel en una votación. El procedimiento es simple y en principio parece correcto y suficiente, dando una falsa sensación de transparencia y eficiencia.

La propuesta se basa en utilizar junto con el equipo de votación electrónica una impresora de papel en la cual una vez seleccionado el voto y antes de su emisión

se reproduce el mismo en una papeleta que se imprime a la vista del votante para permitir la verificación del mismo. Este proceso se produce en algunos casos fuera del alcance del votante, habitualmente detrás de una caja de cristal o plástico. Finalmente, cuando el votante verifica la coincidencia entre el voto seleccionado en el equipo electrónico y la papeleta, esta cae en la urna que recoge todos los votos en papel para un recuento manual si fuera necesario auditar la votación.

Métodos como el VVPAT, presentan la posibilidad del recuento manual ya que se imprime la papeleta que posteriormente se deposita en una urna convencional, aumentando las garantías de seguridad en los procesos de votación al incrementar la transparencia que no existía en las "cajas negras" de los DRE, pero ofrece una débil protección de la integridad del voto, puesto que las papeletas impresas pueden ser eliminadas, sustituidas o ser marcadas por los votantes y de esta forma dar pie, si se tuviera acceso a ellas, a impugnaciones o coacciones en cadena. Es importante determinar previamente al depósito del voto, si el voto impreso coincide con la intención de voto y establecer un mecanismo de cancelación, lo que complica este método. Sólo si el votante tiene la oportunidad de revisar el documento generado antes de dejarlo en la urna clásica, se estará procediendo de una forma correcta. De esta manera este método proporciona una posibilidad de auditoría si recontamos los votos en papel para comprobar su coincidencia con el recuento electrónico; claro que en este caso hemos complicado sin necesidad el procedimiento de votación. Se justifica su uso apoyándose en el argumento de que no es necesario auditar todas las urnas y que es suficiente una muestra. El problema es determinar correctamente ésta y considerar qué ha de hacerse en caso de discrepancia. Un poco más adelante analizaremos otros aspectos que han puesto en duda este método [76] [77]. Este sistema se utiliza en Venezuela y en algún estado de Méjico [3] [5].

En la práctica este desarrollo tiene diversos tipos de problemas [78] [5] [32] como los que vamos a señalar a continuación. En cualquier caso, en la impresión de la papeleta por un elemento del sistema de votación que suele ser una impresora, puede producirse un error o divergencia entre lo que el votante quería expresar en su voto y el valor que finalmente ha sido impreso. En este caso ha de habilitarse un procedimiento para anular dicho voto y proceder de nuevo a iniciar la emisión del mismo. También ha de estudiarse la posibilidad de una falta de coincidencia entre el resultado del recuento digital de los votos y el manual en aquellos casos que se utilice para su verificación.

Estos sistemas basados en VVPAT han sido estudiados en ensayos cuidadosamente diseñados para verificar su usabilidad y transparencia. La idea central es verificar que los votantes puedan comparar que su voto en la pantalla del equipo coincide con el registrado en un pequeño trozo de papel. Sin embargo los estudios nos dicen que no es así. Este es el caso de la tesis doctoral de Sarah Everett de la Rice University del año 2007 en el que demuestra que dos terceras partes de los votantes no se percatan de la desaparición de información en sus votos [76].

Por otro lado Ted Selker del CalTech/MIT en el 2004, identificó dieciocho problemas diferentes con los equipos de votación dotados con VVPAT: desde

problemas con las impresoras, el papel, el formato de impresión, incremento del tiempo de votación y problemas con la usabilidad y accesibilidad del equipo [77].

La idea que subyace a este tipo de soluciones es algo así como: "tenemos la posibilidad de realizar una verificación de la urna si fuera necesario" y el problema es determinar por parte de los administradores del proceso electoral cuándo "es necesario" y en todo caso esto produciría un aumento en el tiempo de recuento que acabaría con una de las principales ventajas de la votación electrónica.

A pesar de todo, el proceso de auditoría tiene aspectos poco claros, es complejo de implementar, poco accesible y caro. En este sentido añadir una impresora a cada urna electrónica encarece el producto y le confiere una mayor probabilidad de fallos. Por otro lado no está claro si la impresión en papel es suficientemente accesible y usable. Tampoco está claro cómo proceder en caso de detectar por parte del votante, si lo detecta, que el voto en papel no coincide con su elección electrónica: ¿invalidamos el voto? ¿Se le permite votar de nuevo? ¿Pierde el votante el anonimato? Por si no fuera suficiente, el procedimiento está abierto a ser utilizado como método de coacción si el votante se ve obligado a realizar una fotografía de su voto en papel antes de depositarlo en la urna, aspecto que no ocurre en una pantalla ya que en todo momento puede dar marcha atrás a su elección, no dejando constancia de su voto real (si el sistema está correctamente diseñado). Por último, si fuera necesaria la auditoría, ésta sería muy lenta al tener que realizar el recuento de forma manual [79]. Incluso algunos autores han demostrado que puede no funcionar correctamente [80].

Es por ello que podemos concluir que el voto electrónico con VVPAT añade una complejidad y un coste a las DRE y en cambio no facilita las tareas de observación externa, ni garantiza que los resultados obtenidos coincidan con la voluntad de los votantes [81].

2.6.2. Auditoría extremo a extremo (E2E) o indirecta mediante recibo

A partir del desarrollo de la tesis de Ben Adida [38] dirigida por Ronald Rivest denominada *Scratch & Vote* [82], se ha abierto la posibilidad de que el proceso de auditoría sea realizado por el propio votante de una forma indirecta y con un ingenioso procedimiento basado en un sistema criptográfico de clave pública de Paillier [83] y utilizando el homomorfismo en contadores desarrollado por Baudron et al. [84]. La idea se sustancia en el uso de una "papeleta desafío" que contiene un código de barras y un identificador alfanumérico corto que el votante utiliza antes de proceder con la votación real y con el objeto de poner a prueba todo el proceso. Además se imprime un recibo de votación que podrá ser utilizado en cualquier momento, tanto por el votante como por la organización, para comprobar que el voto ha sido tenido en cuenta en el recuento pero sólo el votante podrá y tendrá que recordar el código visualizado en el momento del depósito del voto,

evitando de esta forma todo tipo de coacciones y venta de votos al no poderlo demostrar.

Por otro lado y de forma simultánea dispondremos de un *tablón de anuncios electrónico (bulletin board)* que podremos consultar a través de terminales dispuestos a tal fin en el colegio electoral y por Internet para verificar que mi voto ha sido depositado en la urna electrónica. Hasta aquí hemos hecho posible la auditoría personal antes del recuento. Después del mismo y una vez hechos públicos los resultados finales, podré volver a verificar que mi voto ha sido tenido en cuenta mediante el tablón de recuento de similares características que el anterior.

Así, tanto de forma individual como colectiva podemos verificar el proceso de votación electrónica en todo momento y saber que mi voto ha sido contabilizado correctamente ya que mi recibo de votación me permitirá comprobar en el listado del tablón de recuento su presencia y mediante el código que apareció en pantalla en el momento de emitir el voto sabré que se ha sumado en la opción correcta.

Con este procedimiento estamos exentos de auditar los diversos elementos que componen el sistema de votación y utilizamos una auditoría de extremo a extremo con las ventajas de sencillez y rapidez que esto supone [70]. Al menos esta es la opinión de los expertos que han desarrollado las soluciones que vamos a analizar y comparar en esta tesis.

Es importante reseñar que aunque en la literatura anglosajona la palabra utilizada sea auditar (*audit*), he preferido aplicar desde este momento una traducción más cercana a la realidad y de esta forma utilizaré "comprobar" o "verificar" para aludir a estos procesos.

3

3.Antecedentes y estado del arte

"¿Qué sabe el pez del agua
dónde nada toda su vida?".

Albert Einstein

3.1. Breve Historia

Sin duda el libro más completo sobre la historia de la votación electrónica es el recientemente publicado por Jones y Simons [44] aunque en su mayor parte trate sobre los Estados Unidos. En el mismo podemos leer que existen históricamente cinco fases en la historia del voto electrónico que podríamos denominar así: máquinas mecánicas, equipos basados en un ordenador, DRE (Direct Recording Equipement), sistemas que proporcionan verificabilidad por medio de papel (VVPAT) (Voter Verified Paper Audit Trail) y sistemas con verificación de extremo a extremo (E2E).

3.1.1. Génesis del voto electrónico

Puede parecer que los intentos de utilizar las Tecnologías de la Información y de las Comunicaciones (TIC) en los diversos aspectos del voto electrónico (VE) son recientes, pero no es así. De hecho una de las primeras aplicaciones de las tecnologías electromecánicas de finales del siglo XIX fue su uso para el ejercicio del VE y del recuento de votos posterior. Así Thomas Alva Edison en 1869 firmó una aplicación de patente (nº 90646) para un sistema de grabación de voto eléctrico el cual luego sería utilizado en su primera patente. En 1892 Jacob H. Myers diseñó la AVM (Automatic Voting Machine) que se utilizó en varias ocasiones en el estado de New York. Era una máquina basada en mecanismos de levas que se siguieron utilizando posteriormente en otras máquinas similares (Davis y Boma machines). Con la aparición de los primeros computadores a mediados de los años cuarenta, se retomó la posibilidad de utilizarlos

para el VE y varios prototipos vieron la luz a mediados de los 60. Más tarde, aquellos se han venido utilizando de modo generalizado en todo el mundo para el recuento de votos y el cálculo de resultados finales. La idea de modernizar los procesos electorales utilizando tecnologías basadas en la electrónica proviene de pensadores como Fromm (1955), Fuller (1963), Arterton (1987) y Rheingold (1993). En la actualidad es raro el país que no haya intentado desarrollar pruebas de voto electrónico con diversos tipos de soluciones y tecnologías.

3.1.2. Los equipos de votación mecánicos y electro-mecánicos

Los equipos de votación puramente mecánicos fueron utilizados a finales del siglo XIX en el estado de New York. El proceso de votación se realizaba en privado gracias a una cortina que la cubría. El votante indicaba su elección mediante unas palancas organizadas en filas y columnas y una vez manipuladas con sus preferencias tiraba de una palanca de votación que incrementaba los contadores oportunos y que solo al final del período de votación se abrían rompiendo un precinto. Posteriormente y en los años sesenta se introdujeron las tarjetas perforadas que permitían un voto mucho más extenso al disponer de hasta 200 opciones. La perforación de las tarjetas se realizaba alineando cuidadosamente la tarjeta de referencia con todas las opciones posibles y la propia tarjeta del votante que perforaba manualmente para posteriormente introducirla en una urna. Al final del período de votación las tarjetas eran leídas mediante un equipo electromecánico. El principal problema, dejando aparte la escasa usabilidad del sistema, era que si la perforación no se realizaba con la presión suficiente el trocito de papel no se desprendía y en el momento de la lectura volvía a tapar el agujero impidiendo el correcto recuento. Este defecto impidió el correcto recuento en el estado de Florida en las elecciones presidenciales del año 2000 que fue esencial para que Gore no se impusiera a Bush. Esto suscitó un profundo debate y algunos estados propusieron la introducción del siguiente paso en sistemas electrónicos de votación, los que incluían un ordenador para permitir el recuento electrónico.

3.1.3. Informatización de la máquina de votación

Inicialmente aparecieron a finales de los años sesenta los equipos basados en el recuento por lectura óptica. Incluso en nuestro país existe un desarrollo denominado Demotek realizado en el País Vasco [72]. Estos sistemas utilizan unas hojas de votación especialmente diseñadas para el proceso electoral y en las que figuran las diversas opciones con una celdilla especial que ha de ser rellenada con un bolígrafo especial de forma similar a como se rellenan los exámenes de tipo test automatizados. Posteriormente la hoja se pasa por un lector especial que realiza el reconocimiento de las marcas y actualiza los contadores únicamente si la lectura es correcta, devolviendo la hoja al votante si no es así. Si la lectura ha sido correcta, la hoja cae en la urna que está debajo del lector con objeto de servir de verificación si fuera necesario. Todavía hoy en día estos lectores ópticos siguen siendo utilizados en algunas zonas de los Estados Unidos [85]. Aun así este tipo de máquinas requieren de una inversión específica en las papeletas para adaptarlas a cada estilo de votación y pueden producir retrasos por errores en la lectura.

Otro paso que posteriormente se ha revelado como nefasto, fue la introducción de equipos de votación electrónicos, con o sin pantalla táctil, que guardaban los votos en su memoria sin ofrecer ningún tipo de garantía para al final de la sesión de votación ofrecer los resultados del recuento. Es evidente que utilizar un ordenador para hacer un simple recuento no puede considerarse complejo de programar pero la gran cantidad de

amenazas, manipulaciones y malfuncionamientos han puesto en jaque a estos sistemas. Los resultados prácticos a lo largo de estos últimos años han sido muy reveladores y de todo ello se ha sacado una conclusión: han generado una gran desconfianza. En los últimos años han sido disfrazados con las siglas DRE (Direct Recording Equipement o Direct Recording by Electronics) y vendidos como la panacea al resolver algunos problemas de usabilidad y accesibilidad o de evitar el papel. Por el contrario un sinfín de estudios serios han demostrado la posibilidad de un funcionamiento incorrecto, ya sea por errores en la programación o por ataques maliciosos, que nos llevarían a un callejón sin salida al no poder recuperar la información correcta debido a que no se establecen procedimientos de recuperación de errores. Grandes empresas, estados y autoridades electorales se han visto implicadas en procesos electorales sin garantías democráticas e incluso en acusaciones de fraude electoral. Sin duda esta época no ha conseguido generar la confianza necesaria en estos equipos.

Como se ha señalado en el capítulo anterior, el VVPAT planteado por Rebecca Mercuri en 2002 [86] añade una impresora de papel a los DRE, de forma que después de que el votante realiza su elección aparece una papeleta impresa para confirmar su voto y si este no fuera correcto le da la opción de anularlo. En caso de que su voto fuera correcto la impresora corta la papeleta y la deja caer en una urna que permitiría la comprobación posterior al recuento final, todo ello fuera del alcance del votante ya que está detrás de un cristal. De alguna forma este sistema es un híbrido entre las votaciones clásicas en papel y el uso de los ordenadores que encarecen y complican los procesos electorales, aunque introduce un recuento más rápido. De todas formas este diseño obliga a una votación y verificación presencial, lo que resulta demasiado rígido y sujeto al correcto funcionamiento de un dispositivo mecánico como es una impresora de papel. Además en los casos en que el voto se deposita manualmente no está exento de riesgos si una papeleta impresa cae en manos de una parte interesada y pone en marcha una coacción en cadena [22] [21], se lleva utilizando en algunos estados americanos desde finales del 2006 [87].

El último paso ha sido propuesto por la comunidad científica con variadas soluciones que convergen en la posibilidad de auditar las máquinas de votación electrónica de forma indirecta en lo que viene a denominarse verificación de extremo a extremo (End to End Voting). Con este tipo de soluciones no es necesario comprobar el correcto funcionamiento de cada elemento de la urna electrónica en cada momento, sino que se verifica el resultado de salida del equipo mediante la publicación de un listado de todos los votos emitidos con un número de registro que permite la verificación del sentido del voto de forma individual y general. En los entornos anteriores solo unos pocos implicados en el proceso electoral, en general las autoridades electorales, podían verificar la votación. En cambio en el caso que nos ocupa cualquiera de los votantes pueden comprobar las entradas y salidas en el sistema mediante pruebas matemáticas descritas como seguras y fiables. Como analogía sencilla se utiliza el protocolo de enrutamiento de las comunicaciones en Internet mediante el cual se hacen llegar los paquetes en los que está divida la información desde un punto de origen a otro destino y se comprueba en los extremos la integridad del mensaje enviado mediante rápidas operaciones matemáticas y evitando los detalles de lo que ocurre en el medio. De la misma forma, en los equipos de votación evitamos tener que preocuparnos de auditar cada uno de los elementos que componen el sistema, aspecto que se ha revelado como muy complejo [58] [88] [89] [5] [90] [91] [21] [92]. Esta solución se consigue mediante un maridaje entre esquemas criptográficos y tecnología electrónica. La criptografía nos permite cifrar los votos para preservar el anonimato, garantizar la robustez e integridad del sistema y generar pruebas para una auditoría pública del proceso de registro y recuento de los votos. En el siguiente capítulo analizaremos estos aspectos.

3.2. Uso mundial del voto electrónico presencial

3.2.1 Visión general

Muchos países en el mundo han considerado el uso del voto electrónico. De ellos una buena parte han realizado pruebas y algunos ya utilizan el voto electrónico de forma vinculante. En Europa, como ahora veremos, se han desarrollado diversos esquemas con pruebas en la mayor parte de los países. Además tenemos a una parte de los antiguos países que formaron la Unión Soviética. Fuera de Europa el uso del voto electrónico está ampliamente desarrollado en la mayoría de los estados de U.S.A., en Brasil, Venezuela y la India, seguidos de cerca por Méjico. También está siendo considerado en buena parte de los países de América Central y del Sur. Vamos a ver con más detalle las experiencias más destacadas en algunos de estos países.

Suiza, que aunque en Europa no forma parte de la Unión Europea, es un ejemplo a seguir por el desarrollo en la implantación del voto electrónico remoto o telemático. En este país, dividido administrativamente en cantones, se llevan a cabo consultas de forma continua y era muy utilizado el voto por correo. Posteriormente en algunos de los cantores se pusieron en marcha pruebas de voto telemático utilizando diversos métodos y durante varios años. Estudios posteriores determinaron su uso vinculante, sobre todo después del alto incremento en la participación que se produjo en los referéndums de 2003 y 2004 realizados en Anières, Cologny y Carouge (ayuntamiento de Ginebra) [93]. En 2008 se ofreció la posibilidad de votar a los suizos residentes en el extranjero utilizando la infraestructura del cantón de Ginebra. Hoy la mayor parte de los ciudadanos suizos utilizan y confían en el voto telemático y esto se debe a un adecuado diseño y una lenta implantación [94].

Bélgica fue el pionero del voto electrónico en Europa. En este país es obligatorio el voto a partir de los 17 años y existen siete tipos diferentes de elecciones. Lo utilizaron en el cantón de Verlainer en 1991 con tarjeta magnética y lápiz óptico y hoy en día se sigue utilizando este sistema junto con equipos DRE. En octubre del 2000 ya el 42% de la población votó electrónicamente. En marzo de 2003 votó electrónicamente el 44% del electorado (3,2 millones de ciudadanos). En cualquier caso, este país es muy especial debido a que su sistema electoral es muy complejo, por lo que el uso del voto electrónico es valorado positivamente por la administración electoral [95]. A día de hoy se sigue utilizando con éxito a pesar de haberse detectado alguna vulnerabilidad [96].

Holanda ha llevado a cabo pruebas con estas tecnologías incluyendo el voto por Internet y teléfono. La mayor de ellas tuvieron lugar en junio de 2004 para las elecciones al parlamento europeo. Actualmente se puede votar electrónicamente pero la opinión de los ciudadanos está dividida, sobre todo después de una demostración en directo y por televisión, de cómo se puede modificar una parte del software de la máquina y recibir emisiones radioeléctricas a distancia con información de qué se está votando. La empresa que fabrica la urna (Nepad) garantizó que corregiría los errores. Esta misma máquina con pequeñas variantes se está utilizando en pruebas en Alemania y Francia. También en este país se utilizó un sistema de votación telemático que permite la auditoría E2E, conocido como RIES, que permitió la participación de 20.000 votantes ausentes en las elecciones municipales en el 2006. En 2008 se suspendió su utilización debido a la aparición de fundadas dudas sobre el incumplimiento del requisito del secreto del voto [97].

En **Inglaterra** se han desarrollado pruebas a nivel municipal desde el 2000 [98]. En junio de 2004 se hizo una prueba de voto electrónico en Londres. El proceso utilizado es minucioso y se desarrolla con tiempo, obteniendo de esta forma un avance seguro hacia

un escenario de voto electrónico bien diseñado y correctamente planificado, lo cual no significa que por el camino no aparezcan problemas como lo ocurrido en los comicios municipales celebrados en mayo de 2007 en los que se perdieron una parte de los votos. Un estudio posterior critica la falta de un sistema lo suficientemente riguroso de auditoría que asegure que tanto el hardware como el software que se utilizan están libres de vulnerabilidades, de lo cual ya hemos hablado anteriormente. Estas razones junto con diversos problemas en los pilotos de votación han llevado a este país a abandonar el voto electrónico aunque en los últimos meses se ha planteado la posibilidad de abrir un canal de votación por Internet debido a la muy baja participación de los jóvenes [99].

Escocia es un caso similar al anterior. Además dispone de uno de los sistemas de participación ciudadana (e-petitions) para su parlamento más elaborado, analizado y cuidado de Europa [100].

Irlanda desde el año 2000 ha desarrollado un proyecto elaborado cuidadosamente para introducir quioscos de voto electrónico en todos los colegios electorales para las elecciones locales de junio de 2004. Finalmente y gracias a que el proceso fue totalmente abierto, se emitió un informe por parte de dos destacados científicos que pusieron en duda la fiabilidad del sistema y no se llevó a cabo. Fue abandonado definitivamente en 2009 por decisión gubernamental ya que se consideró que el sistema no reunía las condiciones básicas de funcionamiento democrático [101].

Alemania comenzó sus primeras pruebas de voto electrónico en 1999 pero en ámbitos no políticos y ha elaborado una documentación precisa sobre los requisitos que deben cumplir los equipos involucrados. En septiembre de 2005 se utilizó el voto electrónico presencial para las elecciones parlamentarias de forma vinculante en algunos colegios con éxito desigual. También se desarrolló un sistema de voto por Internet (i-vote) pero no ha sido utilizado para elecciones vinculantes. Posteriormente, en 2009, la Corte Constitucional declaró inconstitucionales los sistemas empleados ya que no se pudo demostrar que cumplieran con los requisitos necesarios [102].

Austria estableció en julio de 2003 un plan para el voto electrónico. Se han desarrollado pruebas de voto por Internet, en paralelo con las elecciones presidenciales en abril de 2004 con una evaluación correcta. En la primavera de 2004 el Ministerio del Interior constituyó un grupo de trabajo sobre voto electrónico [103].

Francia ya en el 2003 utilizó Internet para elecciones para el Consejo Superior de Franceses en el Extranjero (CSFE), pero sin conseguir incrementar la participación. También se ha utilizado voto electrónico en colegios electorales seleccionados, usando para identificarse la huella dactilar integrada en una tarjeta (smart card), para las elecciones al parlamento europeo en 2004. En las elecciones presidenciales del 2007 también se utilizaron urnas electrónicas por parte de 1,5 millones de personas de un total de 44,5 millones del censo. Se registraron problemas de usabilidad sobre todo con los votantes de mayor edad y esto ha llevado al país vecino a replantearse su uso. El debate sobre su uso continúa [104].

Rusia ha desarrollado un proceso de implantación del voto electrónico paulatino y mediante pruebas bien diseñadas. Su sistema está basado en una red de interconexión entre los colegios electorales denominada Vybory y ha sido ensayado en muchas ocasiones con un acertado y equilibrado control de resultados. Esta red admite la conexión de lectores ópticos, DRE e incluso dispositivos para el voto remoto. A finales del 2015 está previsto que el 15% de los colegios dispongan de este sistema. En cualquier caso el problema de este país en opinión de los observadores internacionales y desde las elecciones del 2007, es la falta de garantías democráticas en el diseño de los procesos electorales [105].

Los **Estados Unidos de América** son un caso especial debido a la gran complejidad de su sistema electoral, en el que cada estado e incluso cada condado determinan la forma y los recursos electorales que se van a utilizar. En las elecciones presidenciales de noviembre de 2000, casi el 70% de los votantes utilizó la vía electrónica para emitir su voto, contando con anticuados mecanismos como la tarjeta perforada, aunque también se utiliza el voto mediante lectura óptica (OCR) y los sistemas DRE. En esta ocasión las irregularidades fueron muy importantes, sobre todo en el Estado de Florida debido a problemas con el diseño y lectura automática de las papeletas perforadas [7]. En los comicios nacionales de 2004 en los EE.UU. la mayor parte de los votantes emplearon sistemas automatizados: el 13,7% de los ciudadanos votaron con tarjetas perforadas; el 14% empleó sistemas similares a la manivela de hace más de 100 años; el 34,9% sufragaron en equipos de lectura óptica y el 29,3% empleó para votar equipos desarrollados bajo el concepto de los DRE. El resto lo hizo con urnas clásicas y recuento manual. El mapa actual es sumamente complejo y disperso [69] aunque predomina el voto con DRE y VVPAT. El principal inconveniente de estos sistemas es la confianza ciega que se deposita en los expertos que supervisan los procesos y la falta de mecanismos de verificación, lo que pone en tela de juicio su validez. Uno de los fallos más destacables de estos sistemas es el que tuvo lugar en el estado de Florida, donde la falta de normativa y control, unido a una tecnología obsoleta (tarjeta perforada), propició que en muchos casos no pudieran saber con certeza qué opción era la que habían marcado.

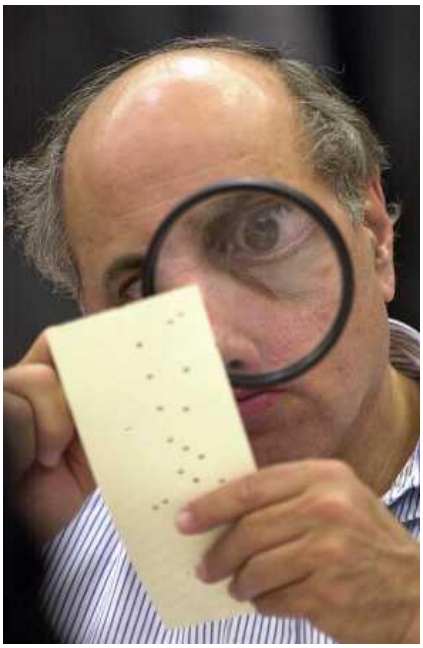


Ilustración 1. Voto en papel perforado (USA) (totallycoolpix.com).

Otro caso muy relevante fue el de compañía Diabold y más concretamente su sistema AccuVote. En el 2004, los profesores de la Universidad Johns Hopkins, Avi Rubin y Yoshi Kohno, analizaron el código fuente y determinaron la falta de seguridad del mismo [21]. Posteriormente se fueron sumando más verificaciones negativas hasta el punto de que el Secretario de Estado de California, Kevin Shelly, retiró el certificado a 14.000 de estas máquinas y ordenó una investigación por supuesto fraude de la compañía. Los informes coinciden: "El uso de código fuente propietario, que está oculto y es complejo en sí, hace que sea extremadamente difícil determinar la ausencia de código malicioso en el firmware".

En los EE.UU. existe un debate muy enriquecedor sobre el uso de la tecnología en los procesos electorales. Desde finales del 2006 funciona en la Universidad Johns Hopkins un centro de estudio destinado a incrementar la confianza en las tecnologías del voto electrónico [106]. El proyecto está destinado a abordar las inquietudes del público con respecto al empleo creciente de urnas electrónicas en los comicios locales, estatales y nacionales. Es importante resaltar que ésta no es una propuesta privada. La iniciativa denominada ACCURATE (preciso), que por sus siglas en inglés significa elecciones correctas, funcionales, confiables, auditables y transparentes, ha recibido 7,5 millones de dólares por parte de la Fundación Nacional para las Ciencias de EE.UU. [107].

Con el respaldo de la Ley denominada Ayuda a América a Votar (HAVA), promulgada en el año 2002 [108], los gobiernos municipales y locales de EEUU están debatiendo sobre la conveniencia de aumentar la tecnología en próximos comicios.

Todo indica que Estados Unidos se desplazó hacia la votación electrónica en las elecciones públicas antes de que la tecnología estuviera lista y que se hizo sin estudios ni pruebas previas. Básicamente, el proyecto, liderado por Avi Rubin, ha analizado las máquinas y la programación de votación electrónica, incluidos los mecanismos de cifrado que se utilizan para garantizar que los electores mantengan su privacidad, así como los métodos usados para verificar que los ordenadores totalicen con precisión todos los votos legítimos [109]; otros miembros del equipo se encargaron de los aspectos legales y de las políticas públicas que han recibido poca atención en la transición a la votación electrónica.

Para intentar disminuir las dudas sobre los sistemas automatizados, los investigadores de la Universidad Johns Hopkins [106] consideran necesario abrir los procesos de prueba de los sistemas a la observación por parte de los ciudadanos y organismos independientes, establecer procesos permanentes de análisis, facilitar los estudios independientes, ejecutar auditorías de las máquinas de forma aleatoria para comprobar que nadie haya manipulado el software utilizado, realizar muestreos en sitios aleatorios y en un número específico de máquinas el día de las elecciones para comprobar que cada sistema registra los votos de manera adecuada, detectar si el código fuente de los equipos ha sido modificado, exigir una revisión de las pantallas en todas las máquinas de votación para minimizar la posibilidad de votos ocultos u otras anomalías y contar con la impresión de un registro físico permanente, independiente del recibo entregado al elector al momento de votar, para la verificación de su voto. Este último aspecto es hoy en día considerado como la solución con mayores garantías, como ya hemos expuesto. Claro que todo esto puede hacer que el proceso automatizado se convierta en más complejo que el clásico, ya que requeriría de una verificación manual sobre el proceso automático, es decir dos procesos en uno y por tanto acabaría siendo más laborioso, lento y caro. Cabe destacar que el profesor Aviel Rubin publicó en el 2006 un libro titulado "Brave new ballot" [92] en el que literalmente dice: "Imagine por un momento que usted vive en un país donde nadie está seguro de cómo se cuentan los votos y no existen registros fiables para realizar un recuento. Imagine que las máquinas cuentan los votos pero nadie sabe cómo lo hacen. Ahora imagine que alguien descubre que estas máquinas son vulnerables a ataques, pero las agencias responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en U.S.A. no necesita imaginárselo. Esta es la realidad del voto electrónico en este país".

Canadá sigue la estela de los EE.UU. en esta materia. Aunque a nivel federal no se utiliza el voto electrónico, sí se hace en las elecciones municipales y locales en algunas ciudades desde 1990. Carece de estándares propios pero utiliza los que su vecino americano va creando. Cada provincia escoge su tecnología y tiene sus propias normas.

Méjico, al igual que otros países, depende de los Institutos o Comisiones Electorales de los Estados para la definición del uso de las diversas tecnologías para el VE. Los Estados de Coahuila, Distrito Federal, San Luis de Potosí y Jalisco tienen urnas electrónicas que ya han sido utilizadas en algunos procesos electorales. El pionero fue Coahuila que en el 2002 desarrolló su propia DRE [5].

Ilustración 2. Urna electrónica de Coahuila (Méjico) (iepcc.org.mx).

En este caso cabe destacar que los desarrollos son propios y los equipos han sido auditados voluntariamente en algún momento después de su fabricación [5]. Son dos aspectos positivos que tienen pocos países.

Ilustración 3. Urna electrónica de Jalisco (Méjico) (proyectodiez.mx).

Venezuela es un caso muy especial, ya que lleva muchos años utilizando con mayor o menor fortuna el voto electrónico basado en DRE. Este país tuvo algún problema por el procedimiento de autenticación del votante mediante lectura de huella dactilar con una máquina denominada "captahuellas" o "cazahuellas" [3], ya que se utilizan las mencionadas máquinas para verificar la identidad de los votantes mediante enlaces satelitales que permiten verificar en "tiempo real" este extremo y existió la sospecha de que eran utilizadas para hacer listas ordenadas de los votantes. Se plantearon problemas muy interesantes debido a la sospecha de que pudieran relacionar las listas de votantes, al pasar en un determinado orden, y el propio voto emitido en un DRE de la empresa Smartmatic, en la que se depositaban en orden secuencial. Por eso en las elecciones del 2005 se retiraron cautelarmente, pero volvieron a ser utilizadas en diciembre de 2006, argumentando que se había roto la secuencialidad utilizando un procedimiento de recolocado seudo-aleatorio de los votos en grupos de diez.

El despliegue tecnológico en las elecciones de este país es uno de los más complejos, ya que además las urnas electrónicas emiten el voto en papel que posteriormente se introduce en una urna convencional (ver ilustración 4) para proceder, en aquellos casos determinados por sorteo, a su recuento manual (verificación por papel). En cualquier caso el recuento resulta lento y complejo debido al diseño del mismo y a la necesidad de realizar la auditoría manual en alguna de las urnas. El proceso está siendo refinado de forma continua.

Ilustración 4. Segundo paso: voto clásico (www.correodelorinoco.gob.ve).

El caso venezolano es un caso muy singular por las circunstancias que concurren. El despliegue de infraestructuras de voto electrónico se produjo en un contexto de fuerte controversia política, en una sociedad muy polarizada y con una elevada dosis de desconfianza institucional fundamentada en factores objetivos y esto nunca es bueno para definir con acierto la implantación de un sistema de estas características. Los resultados del referéndum revocatorio de 2004 fueron duramente contestados y la oposición, dado el tipo de resultados que se produjeron, defendió la tesis de que se había producido una manipulación generalizada sobre el hardware de las urnas electrónicas, en particular sobre las memorias flash que almacenaban los datos de urnas de distritos muy significativos que indujeron resultados favorables para Hugo Chávez. Los expertos adujeron, en función

de los resultados de participación y la secuenciación de los votos, que muchas de dichas memorias podrían haber sido sustituidas por otras con resultados prefabricados [110].

Ilustración 5. Tipos de DRE en Venezuela (smartmatic.com).

Conviene conocer que el papel jugado por la Fundación Carter fue demoledor. Los expertos desplegados por dicha fundación de ningún modo estaban cualificados para valorar las infraestructuras de voto electrónico y los distintos analistas coincidieron en señalar que los resultados de su observación fueron poco esclarecedores [111]. Los protocolos de despliegue de dichas infraestructuras fueron muy deficientes y sobre todo opacos y, para dejar todo dicho, la oposición tampoco adoptó las cautelas que el caso exigía, siguiendo todos los procesos de información, intervención y auditoría que son exigibles. Únicamente se admitió a un grupo de expertos denominados GST (Grupo de Seguimiento Técnico) que elaboraba informes que no eran públicos ni vinculantes.

La opinión del OVE (Observatorio del Voto Electrónico), que declinó su presencia como observador en las elecciones municipales venezolanas del primer trimestre de 2005, es que existen dudas razonables para poner en entredicho la arquitectura física y lógica de las infraestructuras desplegadas [3]. El OVE declinó la petición de la Presidenta del Consejo Nacional Electoral Venezolano (CNE) porque "no se nos proporcionó la información que el OVE prescribió como imperativa para realizar la observación y tampoco se nos garantizaban las acreditaciones reclamadas, que incluían un nivel de acceso suficiente a los centros de totalización de datos y a los centros logísticos que operaban con las urnas electrónicas". Se acudió al sempiterno argumento de los derechos de propiedad intelectual de la empresa proveedora, para no aportar la arquitectura lógica de los sistemas que soportaban el cómputo y almacenamiento de los votos en las urnas electrónicas, ni el código fuente correspondiente a las distintas etapas del proceso, desde la identificación de electores hasta el recuento, pasando por la captura del voto. Este sistema no ha sido nunca auditado de forma pública, al no haber permitido a los expertos el acceso físico a esta urna ni a los detalles técnicos.

En las últimas elecciones del 2013 se incluyó la lectura de las huellas dactilares para la autentificación del votante en la propia red de votación suscitando aún mayor controversia. Además el ciudadano deposita el voto en papel generado en la DRE en una urna convencional, con lo que podría escamotear la papeleta y producir una cadena de coacciones, también denominado "voto controlado en cadena". Este proceso comienza con la posesión de una papeleta del candidato al que deseemos beneficiar y se verifica su depósito en la urna extrayendo otra nueva con la misma selección.

Brasil aprobó en octubre de 1995 una nueva Ley Electoral en la que se definieron las directrices del voto electrónico con la intención de reducir el fraude electoral y minimizar el tiempo de escrutinio, lo cual está plenamente justificado por el número de electores y la complicada orografía del país. La votación se lleva a cabo a través de una especie de cajero automático, en el que van apareciendo los candidatos y en la que los votantes pueden realizar su selección oprimiendo un botón. Al concluir la jornada electoral, se bloquea el equipo mediante una clave y se imprimen los resultados, a la vez que se obtiene una copia de los mismos sobre un soporte digital que se traslada inmediatamente a un Centro de Recuento para su tratamiento o para ser enviado por enlace satelital, si el centro de votación estuviera muy alejado, al punto habilitado más cercano. La urna electrónica fue el único método de votación en las elecciones a Presidente de la República en octubre de 2002 y fue empleado con éxito por 115 millones de votantes.

Este es otro caso especial ya que debido a su complicada orográfica y al historial de manipulaciones y fraudes electorales, forzaron la aparición del voto electrónico como única salida viable. Para darnos una idea, ya en las elecciones municipales de octubre del 2000 votaron electrónicamente 109 millones de ciudadanos. Además se dio la oportunidad de votar a los analfabetos (20 % de la población) mejorando y adaptando la usabilidad del equipo.

Ilustración 6. DRE de Brasil con lector de huellas (votodigital.wordpress.com).

El sistema utilizado es una urna electrónica con teclado de desarrollo propio. La experiencia en este país demuestra que el voto electrónico ha reducido de forma muy importante el voto nulo. Debido a que se vota simultáneamente para tres niveles de representación administrativa se ha incrementado la participación. A partir del 2008 se incorporó a la urna un lector de huellas para la identificación del votante, lo que ha incrementado las dudas sobre el respeto al secreto del voto. En el 2010 la utilizaron 10 millones de brasileños y en el 2018 estará concluido su despliegue en todo el país de este nuevo equipo.

En cualquier caso, en el año 2012 el profesor Diego Aranha y su equipo de la Universidad de Brasilia consiguieron "hackear" la urna electrónica de su país [40]. Si a esto se le añade que, en enero del año 2013, un hacker demostró en directo en Río de Janeiro cómo acceder a la intranet de la red del Tribunal Electoral de esta ciudad y manipular los resultados sin ser detectado [112], hace que las dudas sobre los procesos electorales brasileños se incrementen. Así podemos establecer que el sistema necesita ser mejorado para generar la confianza necesaria en el electorado. A pesar de todo, este país

es ejemplo de uso adecuado del VE ya que el voto convencional generaba aún más inconvenientes que éste basado en tecnología.

Ilustración 7. DRE brasileña básica (votodigital.wordpress.com).

India es otro caso excepcional tanto por el número de electores, 668 millones en las últimas elecciones, como por ser pionera en el uso del voto electrónico (¿alguien ha pensado en hacer papeletas para todos estos electores con la multitud de partidos políticos que se presentan?). Ya en el año 2004 se distribuyeron por encima de un millón de EVM (electronic voting machines) que suministraron dos empresas del propio país, con un diseño sobrio, un coste de fabricación reducido, pero de manejo poco claro. La puesta en marcha del voto electrónico en todo el país se hizo de forma paulatina y comenzó en 1989. De esta forma se fue aprovechando la experiencia para aumentar año a año el número de máquinas.

Ilustración 8. Aspecto de la votación en la India (indiaevm.org).

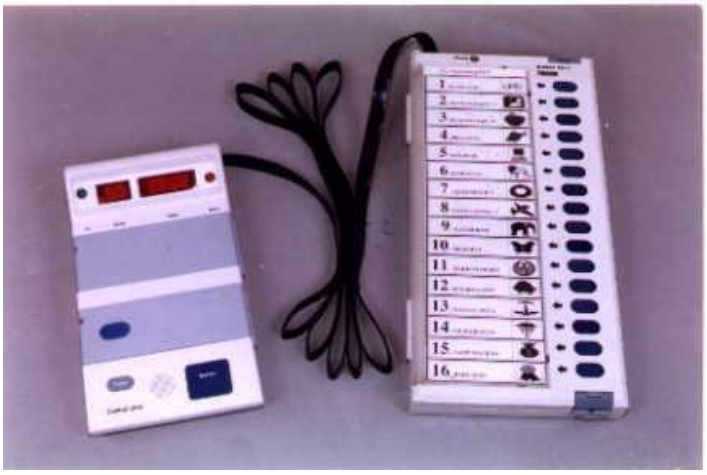


Ilustración 9. DRE de la India (indiaevm.org).

Éste podría ser un buen ejemplo de cómo hacer bien las cosas, sobre todo si tenemos en cuenta que el voto tradicional en este caso sería muy complejo por no decir inviable, debido al elevadísimo número de electores y de opciones políticas, a la arcaica red de comunicaciones y a la enorme extensión del país. Pero en el 2010 el profesor Alex Halderman de la Universidad de Harvard demuestra que las EVM no garantizan la imposibilidad de manipulaciones y hace una demostración de cómo modificar los resultados [29]. Más que nunca tienen sentido las palabras de David L. Dill, que es catedrático de la Universidad de Stanford y presidente fundador de la asociación Verified Votting Foundation, asegurando que el verdadero propósito de unas elecciones no es que los ganadores asuman que han ganado, sino convencer a los perdedores de que han perdido. Por todo ello el proceso ha sido puesto en duda e iniciado un período de revisión profunda [113].

Ilustración 10. El Dr. Halderman y sus colaboradores (indiaevm.org).

Australia empezó a utilizar máquinas de voto electrónico en las elecciones parlamentarias de octubre de 2001, que fueron usadas por más de 16.000 votantes. Ya en

2006 el gobierno del Estado de Victoria introdujo en las elecciones estatales una prueba general con voto electrónico. Posteriormente la Comisión Electoral Australiana ha decidido introducir en 29 localidades el voto electrónico para que puedan utilizarlo 300.000 discapacitados visuales. También se han desarrollado pruebas de voto remoto a la que tuvieron acceso los militares y personal civil desplazado fuera del país en misiones oficiales. Por lo que sabemos el proceso está siendo llevado a cabo lentamente y con acierto pero no sin problemas. En noviembre de 2013 surgieron impugnaciones al recuento electrónico de votos y también aparecieron datos del alto coste de este tipo de voto en el país. A pesar de ello y debido a la gran extensión de territorio sigue en pie su uso [114].

3.2.2. Iniciativas europeas

El Consejo de Europa (CoE) constituyó en noviembre de 2002 un grupo de expertos denominados IP1-S-EE [115] para fijar estándares para el voto electrónico (e-enable voting). Posteriormente se constituyeron dos subgrupos, uno de aspectos legales y operacionales y otro técnico. Pero se verificaron muchas más dificultades de las inicialmente esperadas. Cada país expresó expectativas diferentes en marcos legales distintos y con niveles de seguridad que la industria no podía en aquel momento satisfacer. Además la neutralidad tecnológica fue planteada en varias ocasiones en el núcleo de la discusión. El principal avance fue reconocer la necesidad de una cooperación muy estrecha entre los expertos legales y los técnicos. A raíz de estas reuniones se produjo la aparición de unas recomendaciones publicadas en septiembre de 2004, por parte del Consejo de Ministros del Consejo de Europa, denominadas Rec(2004)11 [116]. Estas se desarrollan sobre dos principios generales: el voto electrónico ha de ser tan fiable y seguro como un proceso de votación en el que no se utilice tecnología y, además, debe ser un canal adicional y opcional de voto, nunca único. La principal iniciativa dentro de la Unión Europea en relación al desarrollo de los denominados sistemas de voto electrónico viene reflejada en esta recomendación Rec(2004)11 . Dicha recomendación propone un conjunto de medidas que deben adoptar aquellos países miembros que decidan implantar métodos de sufragio alternativos a los existentes en la actualidad. Curiosamente, buena parte de las experiencias europeas puestas en marcha posteriormente no han seguido estas recomendaciones [117] e incluso expertos en la materia las han matizado [118].

Los objetivos de la recomendación y el conjunto de normas que la componen son:

- Salvaguarda de los principios consignados en el código de buenas prácticas electorales aprobado en la Resolución 1320 (2003); principios que dictan que un sufragio deberá ser de carácter universal, único, libre, secreto y directo.
- Asegurar la confianza de los ciudadanos en los sistemas de voto electrónico.
- Fomentar la interoperabilidad entre los sistemas de voto electrónico.

La recomendación atañe a la celebración de aquellos procesos electorales o referéndums en el seno de la Unión Europea si bien cada estado miembro podrá adaptar, en función de su regulación específica, la aplicación de la recomendación. Su desarrollo se basa en los principios de carácter legal, operativo y técnico que deben regir en la celebración, ya sea de elecciones o referéndums, en los estados miembros y en la propia institución europea.

En relación con los principios de sufragio universal y único, los sistemas para la emisión del voto han de ser accesibles para el conjunto de la ciudadanía y en especial para aquellos colectivos que presenten algún tipo de diversidad funcional. Asimismo deberán

existir procedimientos que aseguren la unicidad del voto emitido por cada persona autorizada a hacerlo.

En lo que respecta a los principios de sufragio libre y secreto, las autoridades competentes velarán por la celebración de elecciones que respeten los períodos de reflexión previos establecidos así como la ausencia de elementos condicionantes durante el ejercicio electoral. Del mismo modo, el elector deberá ser informado una vez haya completado el proceso de emisión de su voto, así como una vez se haya completado el escrutinio de los votos emitidos. Con el fin de asegurar la privacidad del voto, los sistemas y procedimientos empleados garantizarán la imposibilidad de asociar los votos emitidos con las personas que los emitieron, ya sea durante el proceso electoral o una vez haya finalizado el mismo. Finalmente el Consejo de Europa publicó un manual sobre voto electrónico en 2010 [119].

3.2.3. Iniciativas y experiencias españolas

España también ha desarrollado pruebas de voto electrónico, pero ninguna de ellas ha sido vinculante ya que no lo permite la legislación electoral. Incluso en febrero de 2005 se desarrolló la primera prueba de voto electrónico por Internet que será analizada a continuación. Tenemos toda una historia con un sabor agridulce. En este sentido hay que reconocer que los fracasos han sido diluidos con una política poco transparente que en nada ayuda a cimentar adecuadamente los avances de este país en esta materia, máxime cuando tenemos empresas y desarrollos de primer nivel en este sector [120] [121] [122].

Destacaríamos las iniciativas del ayuntamiento de Jun (Granada) y de los ayuntamientos de Madrid y Barcelona. Las experiencias de las elecciones sindicales en la Policía Nacional y la prueba no vinculante realizada en el referéndum sobre la Constitución Europea de febrero de 2005.

Si hay alguien al que se le puede considerar pionero en el intento de poner en marcha el VE en España es al alcalde de Jun, José Antonio Rodríguez, que ya en el año 2001 inició una experiencia que la prensa vino a denominar "teledemocracia" y "ciberdemocracia" [123].

En junio de 2004 el Ayuntamiento de Madrid convocó a los cerca de 140.000 habitantes del distrito centro de Madrid para expresar su opinión sobre cuestiones relacionadas con sus competencias, con la ayuda tecnológica de la empresas Scytl y H.P. [124]. En este caso hubo destacados informes [67] en los que se pidió prudencia a la hora de poner en marcha procesos de votación electrónica.

En mayo de 2010 se puso en marcha una experiencia en Barcelona para decidir qué hacer con la Diagonal. Esta fue una votación telemática a través de un portal web, con un censo cercano al millón y medio de ciudadanos durante cuatro días. Posteriormente también se admitió el voto presencial. Este asunto acabó con la dimisión del primer teniente de alcalde del Ayuntamiento por errores en la puesta en marcha y desarrollo del VE en esta consulta [125]. Las empresas implicadas (Indra y Scytl) tuvieron que justificar los problemas que aparecieron durante esos días.

De estas pruebas se pasó a experiencias vinculantes aunque en ámbitos de un nivel inferior al electoral ya que jurídicamente y a día de hoy no son posibles. Este fue el caso de las elecciones sindicales de junio del 2011 en la Policía Nacional que también acabaron con polémica. En este caso fue Telefónica la implicada y la prensa lo calificó de "pucherazo" [126]. En cualquier caso tuvieron que repetirse posteriormente y se solicitó una auditoría que, como ya hemos justificado, poco puede aclarar en este ámbito.

3.3. Experiencias de voto telemático o remoto

La Unión Europea desarrolló un proyecto denominado EU CyberVote Project entre los años 2002 y 2003 [115]. El objetivo era verificar las garantías de privacidad y seguridad en una votación en línea sobre Internet utilizando terminales fijos y móviles. Fue desarrollado por empresas de telefonía, tecnología y universidades. Las conclusiones de este proyecto son que el prototipo diseñado por CyberVote [127] funciona en condiciones normales tanto desde terminales fijos como móviles, como se puso de manifiesto en varias pruebas, pero es imposible garantizar su fiabilidad en votaciones reales y en ambientes no controlados, es decir, allí donde están presentes los grandes riesgos en materia de seguridad de Internet. Las experiencias de este tipo que han sido realizadas con valor vinculante se han desarrollado en contadas ocasiones.

Las escasas experiencias y los problemas de seguridad en el voto remoto o telemático, un voto que necesita reforzar todas las cautelas en los centros de cómputo y donde la arquitectura lógica desempeña un papel crucial, limitan su uso de forma vinculante en el mundo. En opinión del OVE son pruebas inapropiadas en su formulación y en su ejecución que no debieron producirse ni siquiera en grado de hipótesis dado que no cumplen los requisitos legales que son propios de una consulta electoral en determinados ámbitos. Han constituido pasatiempos que han llegado a experimentarse al amparo del nivel de desinformación de las autoridades electorales de cada país y de intereses ajenos al derecho electoral.

En definitiva, es añadir a todas las desconfianzas que ya de por sí tienen las infraestructuras presenciales del VE, las propias de Internet. En este sentido la literatura que pone en duda la seguridad del voto telemático es muy amplia. [128]

En **Estonia** se ha utilizado la posibilidad del voto por Internet en las elecciones municipales del 2005 y del 2009 y en las presidenciales del 2007 y del 2011. Ya en el otoño del 2005 se realizó una prueba piloto avanzada en unas elecciones locales, utilizando *smart cards* con firma electrónica para la identificación del votante. Posteriormente en las elecciones parlamentarias del 2007, 30.275 personas votaron por Internet (3,5% de la población) [129]. En cualquier caso este es un caso muy especial y difícil de extrapolar, debido a la alta penetración de Internet en la sociedad y a la posibilidad de utilizar la tarjeta de identificación con infraestructuras PKI. En este caso el voto remoto no es el único admitido e incluso podía votarse varias veces teniendo validez el último emitido que podía ser por el método tradicional que también estaba habilitado. Es lo que se denomina multicanal. En el 2011 la participación por medio del voto telemático fue de poco más del 15%. En mayo de 2014 un grupo de expertos encabezados por el Dr. Halderman demostró que el sistema de voto remoto en este país no era seguro e instó al Gobierno a abandonar el sistema [130].

En **Noruega** se desarrollaron pruebas de voto por Internet durante las elecciones de 2011 y 2013. Después de su evaluación se concluyó que no se había incrementado la participación pero sí un consenso entre ciudadanos y expertos en cuanto a que el entorno de votación estaba poco controlado [131] [132].

Corea del Sur es un país sumamente preocupado por desarrollar su democracia de una forma abierta, directa y transparente. Por ello la Comisión Nacional Electoral decidió en enero de 2005 establecer un plan de desarrollo de voto electrónico remoto utilizando la telefonía móvil. El proyecto concluyó en 2012 y a pesar del éxito en participación y ahorro en el desarrollo de las diversas elecciones han surgido opiniones en contra por las débiles garantías de seguridad del sistema [133].

Finlandia utilizó en las elecciones municipales de octubre de 2008 equipos tipo DRE conectados a Internet y suministrados por Scytl. Debido a defectos en el diseño de

la usabilidad del sistema, más de 200 electores no pudieron registrar sus votos y la Corte Suprema obligó a repetir las elecciones [134].

Un ejemplo de uso estudiado y que se ha ganado la confianza del ciudadano es el ya comentado de **Suiza** donde se utiliza en los referéndums desarrollados en algunos cantones de forma habitual con objeto de conocer la opinión del ciudadano y elegir propuestas.

En **Estados Unidos** se ha utilizado en las elecciones en Alaska y en la experiencia con el personal del ejército fuera de su país, denominado SERVE [135]. El ejército de Estados Unidos desaconsejó el sistema por deficiencias severas en la arquitectura lógica y los bajos niveles de seguridad. La exposición a ataques de toda la arquitectura lógica fue muy censurada y posteriormente contestada por los expertos del Pentágono. El sistema esperaba 100.000 votos en una primera fase para llegar a 6 millones, con un coste estimado de 24 millones de dólares. Después de un análisis de su seguridad por parte de David Jefferson, en el que se ponían en entredicho muchos de los aspectos de seguridad del sistema, el proyecto se detuvo [136]. Existen otras iniciativas de voto telemático que pueden igualmente ser consideradas, ya que reúnen las condiciones básicas y necesarias. Este es el ejemplo de Helios de Ben Adida y su equipo. [137]

España también ha desarrollado pruebas de voto telemático, pero todas ellas no vinculantes ya que no lo permite la legislación electoral. En febrero de 2005 se desarrolló la primera prueba de voto electrónico por Internet que resultó ser un fracaso técnico y de participación. La prueba se desarrolló con la mediación de Indra, sobre un censo de dos millones de votantes y utilizando ordenadores ubicados en dependencias cedidas por los municipios, uno por provincia. Los censados podían dirigirse a estos lugares y usar el ordenador para votar de forma paralela y no vinculante en la consulta sobre la Constitución Europea o recoger un código para votar desde su domicilio. La participación no llegó a los 11.000 votantes y por si fuera poco el OVE emitió un duro informe sobre las irregularidades técnicas detectadas [138]. También en nuestro país se ha desarrollado Votescript, un producto completo de voto telemático seguro realizado por el Dr. Carracedo y su equipo. [24] "Incluye la realización del análisis, la definición y la implementación de un sistema capaz de soportar los diferentes pasos y elementos existentes en un proceso de votación telemática, abarcando desde el proceso de emisión del voto hasta el de recuento y posterior verificación de los resultados."

3.4. Conclusiones de las experiencias mundiales

De todo lo expuesto podemos extraer varias conclusiones:

- En la corta historia del voto electrónico se han producido importantes cambios en las tendencias de su utilización. El primer y principal impulso se produjo en Estados Unidos a partir de las elecciones presidenciales del año 2000 y en el mismo país tuvo lugar un brusco cambio de tendencia en el año 2006 debido a diversas vulnerabilidades y sospechas que en esta tesis aparecen mencionadas. En el año 2008 Holanda decide suspender las pruebas de *e-voting* y un año después Alemania lo declara inconstitucional. Ese mismo año Irlanda descarta el uso de los DRE en las elecciones. En el 2002 la Dra. Mercuri propone la solución basada en VVPAT y en el 2005 comienzan a proponerse soluciones del tipo E2E que continúan hoy en día. Está claro que la controversia con el uso de estos sistemas sigue abierta.

- En muchos países no se han resuelto algunos de los aspectos del voto electrónico (legal, tecnológico, social, político) debido a que no se han explicado claramente las ventajas y el interés público.
- No hay tendencias únicas en el voto electrónico, incluso en los países con mucha experiencia. Hay países que comenzaron con fuerza y acabaron prohibiéndolo (Alemania) y hay otros que no pueden pensar en sus elecciones sin la ayuda de las TIC (India y Brasil).
- Los países que han intentado implementar sistemas a gran escala, sin debate previo ni transparencia suficiente, se han encontrado con la oposición de varios sectores. Se producen cambios de opinión de forma continua en este tema, lo que podría indicar que no ha sido diseñado ni puesto en marcha de forma adecuada. Los mejores desarrollos se han obtenido gracias a una estrecha colaboración y entendimiento mutuo entre los expertos tecnológicos, los jurídicos, los legisladores, políticos y el público en general. Pocos países han sabido dirigir y desarrollar de forma adecuada el proceso de introducir el voto electrónico (Suiza, Rusia).
- Si se pretende generar confianza en el electorado es necesario planificar la introducción y desarrollo del voto electrónico con transparencia, esfuerzo y objetividad.
- Es necesario hacer un esfuerzo en la usabilidad de los sistemas, así como en la calidad de los equipos y aplicaciones utilizadas. La colaboración entre los estados y las universidades podría mejorar el diseño de las urnas electrónicas y minimizar costes.
- Es necesario determinar qué es preferible para el electorado: un proceso clásico, que podría ser igualmente vulnerado y al que se le añaden tiempos de recuento muy largos y por tanto sospechas de manipulación, o bien, este tipo de soluciones que se caracterizan por un rápido resultado y que aunque mejorable, permite el sufragio de todos y un recuento rápido que reduce las susceptibilidades de manipulación. Compleja decisión en la que, considerando que ninguna de las dos es perfecta, hay que decidirse por aquella que menos lesione los principios democráticos. Es imprescindible generar CONFIANZA en los ciudadanos y ésta no se consigue sin transparencia, formación, debate público y tiempo.

4

4.Análisis y comparativa de las soluciones más significativas de voto electrónico basadas en verificación E2E

4.1. Introducción

En los últimos años se han propuesto varias soluciones que permiten mantener el anonimato, asegurar la fiabilidad y poder garantizar estos extremos con un proceso de verificación que no suponga un esfuerzo añadido al protocolo de votación o al menos así lo intentan justificar sus autores.

Las deficiencias descritas y la búsqueda de soluciones que acerquen la votación real a la ideal, motivaron el desarrollo de los sistemas de votación verificables de extremo a extremo que se presentan a continuación.

La primera iniciativa en este sentido es la diseñada por David Chaum en 1981 [139] en la cual propone un proceso electoral en el que cualquier interesado podría verificar que los votos han sido contados correctamente mediante una firma anónima de la papeleta antes de ser enviada por correo electrónico. La solución está basada en criptografía de clave pública y permite ocultar al participante, así como el contenido de su comunicación (voto) a pesar de utilizar una infraestructura no segura de comunicación (Internet). Además la técnica no requiere una autoridad de confianza al disponer de un protocolo que comprueba que el voto proviene de un elector legítimo.

Los sistemas de votación verificables de extremo a extremo (E2E) (End-to-End auditable voting systems) se caracterizan por su rigurosa integridad y gran resistencia a la manipulación del voto. Estos sistemas a menudo emplean métodos de cifrado complejos para elaborar recibos que permitan a los votantes verificar que sus votos han sido contabilizados correctamente sin poner en peligro el secreto del voto. Por esta razón en algunas ocasiones son denominados sistemas basados en recibos (receipt-based systems) [140] [141] [142] [143]. Incluso se han propuesto soluciones para ser utilizadas sobre Internet [64]. Estas propuestas dieron un gran paso adelante con las tesis doctorales de Richard Carback y Russell Fink en el 2010, dirigidas por Alan Sherman [143] [140], aunque el primer paso fue la tesis de Ben Adida en el 2006, dirigida por Ronald Rivest [38].

De acuerdo con la EAC (United States Election Assistance Commission) [68] las características que distinguen los sistemas E2E son las siguientes:

- Cada votante obtiene un recibo en papel que contiene la información necesaria para poder verificar que su voto ha sido grabado correctamente y que esta información no permita revelar a terceros lo que se ha votado.
- El votante tiene la posibilidad de comprobar que su voto ha sido contabilizado. Esta operación puede realizarse por diversos medios, como por ejemplo a través de un sitio web en el que deberá coincidir la información impresa en el recibo con la expuesta en el mismo.
- Tales sistemas no solamente deben garantizar que el voto ha sido correctamente grabado, es decir tal y como fue emitido, sino que fue contabilizado de la misma forma.

Debido a la importancia del derecho al voto secreto, todos los interesantes esquemas de votación E2E también intentan cumplir con otro requisito: que el recibo no permita identificar al votante ni coaccionarle. Ningún votante debe poder demostrar a un tercero cómo votó ni directa ni indirectamente.

Por otra parte, ¿qué es un voto secreto? Hay dos aspectos en esta pregunta: ¿cómo de secreto es el voto emitido mediante este método y qué es exactamente lo que significa decir que los votantes tienen derecho al voto secreto? [144] [145]. Por estas razones también este tipo de soluciones pueden acumular dudas sobre aspectos legales, administrativos o sociales, pero a día de hoy son estas soluciones las más avanzadas tecnológicamente. Las vamos a analizar, evaluar y comparar, con el fin de clasificarlas en función de los criterios más relevantes para el cumplimento de los aspectos esenciales de una votación democrática.

Actualmente y en los sistemas más modernos, es necesario que una máquina imprima recibos a los votantes posteriormente al ejercicio de su derecho al voto. Este método permite asegurar al votante que su voto es contabilizado de forma correcta y conforme con su elección.

Los sistemas de votación que basados en criptografía permiten la verificabilidad de extremo a extremo (E2E), abren la posibilidad de que cualquier votante sea capaz de auditar el proceso de votación por completo y realizar la trazabilidad de su propio voto. Al mismo tiempo, tales procesos de revisión deberían garantizar la necesidad de mantener el anonimato para evitar la coacción sobre el votante.

Algunos sistemas basados en la emisión de un recibo en papel no proporcionan suficiente anonimato ya que el número único que aparece impreso en el voto para asegurar que es legítimo, puede ser rastreable hasta el nombre del votante. En este aspecto, la mayor parte de los autores usan técnicas criptográficas para mantener la identidad del votante en secreto mientras aseguran que todos los votos emitidos son legítimos.

A día de hoy están suficientemente descritas las siguientes:

- PunchScan de David Chaum [146] (2005)
- Scantegrity de David Chaum [147] en sus diversas versiones (sucesor del anterior a partir del 2007)
- ThreeBallot de Ronald Rivest [148] [60] (2006)
- Scratch&Vote de Ben Adida y Ronald Rivest [149] (2006)
- Prêt à Voter de Peter Ryan [61] [150] (2007)
- Bingo Voting de Bohli/Müller/Röhrich [151] (2007)

Existen otras soluciones que se presentan a continuación, justificando su no inclusión en esta tesis.

Helios. Es un desarrollo en código abierto y público que permite generar un proceso de votación remota basado en web [152]. Desarrollado por Ben Adida y su equipo en el 2006. Está basado en un protocolo verificable y sencillo propuesto por Benaloh [153] y ha sido utilizado en varias ocasiones, ya que permite un uso público y sencillo. A pesar de su importancia, el hecho de que sea un sistema de votación remoto lo excluye de este estudio.

Adder. Es una propuesta muy similar a la anterior con la que tiene varios aspectos en común: código abierto y público y posibilidad de verificación por parte del votante. Fue desarrollado por el Departamento de Ingeniería y Ciencias de la Computación de la Universidad de Connecticut por Aggelos Kiayias y su equipo en el 2006 [154]. Utiliza criptografía homomórfica [155] pero el proyecto ha sufrido una parada en 2009. Como en el caso anterior al ser un sistema de votación remota no se estudia en esta tesis.

Votehere, **Scytl Pnyx** y **SureVote** son implementaciones comerciales en mayor o menor grado y en las mismas fechas que las anteriores. En este caso o bien no se dispone de información suficiente para su análisis o está protegida por patentes, lo que no facilita su análisis y por tanto su crítica. Es la razón de no incluirlas.

Otra solución es el **Prime III** [156] que pone el énfasis en la accesibilidad y usabilidad. Sin duda es un excelente trabajo, que pretende mejorar la interacción del votante con la máquina por medio de la comunicación oral proporcionando un canal de comunicación para las personas con deficiencias visuales. En las pruebas reales aparecen limitaciones como el ruido ambiente que causa una gran cantidad de dificultades al sistema de reconocimiento de voz que se utiliza, el cual reconoce la selección del votante mediante un soplo de aire sobre el micrófono. Además este sistema no proporciona ninguna posibilidad de verificación a los votantes, lo que lo excluye de este estudio al no ser un sistema de votación completo y riguroso.

Aparte de las señaladas, no hay muchas más referencias sobre soluciones propuestas en este sentido o al menos no las he encontrado.

4.2. Análisis de las soluciones con verificación E2E

Según lo comentado anteriormente vamos a presentar y analizar los seis sistemas indicados. Todos ellos proporcionan algún mecanismo de verificación E2E y son de tipo presencial.

En cuanto al orden, se ha respetado el de la fecha de aparición, salvo el Scantegrity que por ser una variante del PunchScan se describe inmediatamente después de éste.

4.2.1. Punchscan

4.2.1.1. Origen

Esta solución fue propuesta originalmente por David Chaum y desarrollada en código abierto (licencia BSD) en diciembre de 2005 aunque actualmente el proyecto está integrado en su sucesor, el Scantegrity [157]. Previamente este autor propuso en 1981 el concepto de votación electrónica verificable [139] y una primera propuesta de sistema de votación electrónica utilizando cifrado visual en 2004 denominado Votegrity [158]. Desde el 2011 el Punchscan ha desaparecido como tal e incluso el portal de descargas de su código ha sido eliminado, pasando oficialmente a ser una parte del Scantegrity que veremos más adelante. Por esta razón y debido a la escasa documentación que lo describa con profundidad y claridad, he optado por presentarlo de forma muy básica y solamente con el propósito de reconocer que fue el pionero de los sistemas aunque hoy en día se haya quedado obsoleto.

Esta solución fue presentada al concurso VoComp organizado en 2007 para comparar diversos proyectos de voto electrónico [159] quedando en primera posición. Para ello tuvo que demostrar sus ventajas sobre otras propuestas y entregar un documento riguroso describiendo el sistema, sus especificaciones, el código fuente (abierto), el análisis de seguridad y su autoevaluación [146]. El documento anterior fue posteriormente simplificado y aclarado en alguno de sus aspectos fundamentales, con el objeto de permitir una verificación independiente [160]. Además ha sido utilizada en las elecciones de la asociación de estudiantes de la Universidad de Ottawa (marzo 2007) y en una encuesta sobre privacidad, libertades y computadores desarrollada en Montreal en mayo de 2007.

A pesar de haber anunciado como característica destacable la posibilidad de incorporar audio a este sistema para mejorar la accesibilidad, no fue implementado en ninguna de las pruebas desarrolladas.

Por último, Punchscan ha sido propuesto para ser utilizado para votar por correo pero los problemas derivados de la necesidad de la presencia de una autoridad electoral para verificar la entrega de la papeleta y destrucción de una de las hojas de la misma, del bajo nivel de custodia en el correo, así como la posibilidad de coerción sobre el votante, desaconsejan su uso.

4.2.1.2. Características

Las ideas básicas de esta solución son aportar una auditoría pública pre y post electoral y que el votante obtenga un recibo de votación libre de coacciones. La verificación puede ser realizada por el propio votante, las autoridades electorales y por observadores independientes. Esta comprobación intenta demostrar que el voto ha sido contabilizado como fue emitido y que este recuento se ha desarrollado correctamente y

preservando el secreto del voto. En principio el nivel de cifrado necesario no es muy complejo y por ello es relativamente sencillo de explicar o al menos eso nos dice su autor.

La verificación se puede llevar a cabo sobre todos los votos, por cualquiera, sobre el software y el hardware independiente y utilizando el código abierto.

Como condición necesaria aparece la imposición de que cada papeleta sea única y para ello muestra un número de serie y un diseño irrepetible, lo que sin duda complica su impresión. Con ello se intentan conseguir dos propiedades, la integridad del sistema y el secreto del voto, aspectos que intuitivamente parecen mutuamente excluyentes. Otra característica esencial es el hecho de que se generen el doble de las papeletas necesarias para el proceso electoral, con el fin de poder llevar a cabo un proceso de verificación antes del comienzo del proceso de votación.

El método se basa en un recuento óptico de los votos y el procedimiento no es sencillo de explicar. El votante marca su elección sobre un papel pre-impreso con dos hojas adosadas y no sobre una pantalla. Posteriormente, parte de la papeleta queda en poder del votante, después de ser escaneada, a modo de recibo para ser utilizada en la verificación posterior. El secreto del voto no se ve comprometido ya que no se puede volver a reconstruir sin la información que sólo está en poder de las autoridades electorales. Gracias a esa información, que siempre permanece en privado, se puede realizar el recuento pero también es posible publicar los datos necesarios para que el votante pueda verificar que su voto ha sido contabilizado correctamente sin desvelar su elección. En principio este esquema está dentro de los parámetros propios de un método de votación que cumple con los criterios básicos de unas elecciones democráticas y añade la posibilidad de una verificación tipo E2E [161] [162].

Como descripción básica, el voto tiene dos capas de papel. En la superior, se ven los candidatos con un símbolo o letra al lado de su nombre y a continuación hay una serie de agujeros redondos en la capa superior de la papeleta. Dentro de estos agujeros y en la capa inferior están impresos los símbolos correspondientes a cada candidato pero no relacionados con el nombre del mismo. Ambas hojas tienen el mismo número de serie. El votante dispone de un rotulador de punta gruesa con el que marca su elección, señalando con tinta tanto en la hoja inferior como en la superior. Inmediatamente después se separan las hojas y se destruye mediante una destructora de papel una de ellas en público y de forma aleatoria.

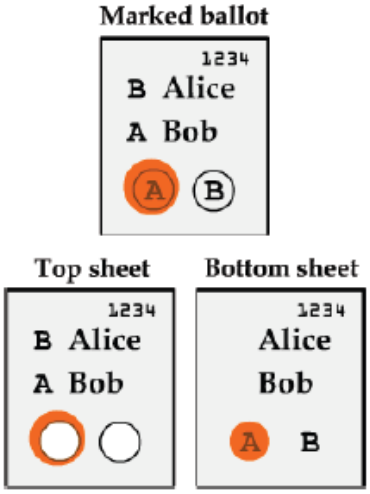


Ilustración 11. Detalle de la papeleta Punchscan [146].

4.2.1.3. Procedimiento de votación

El procedimiento de votación requiere una formación previa del votante y de los miembros de la mesa, disponer de las papeletas y de un soporte similar a una carpeta con una pinza que sujeta las dos hojas de la papeleta. En la zona de votación (colegio electoral) no se accede directamente a las papeletas sino que son entregadas por el personal de la mesa una vez que el votante ha sido identificado y al mismo tiempo se le indica, de forma aleatoria, la parte de la papeleta que ha de destruir posteriormente.

El votante se retira a la cabina de votación y para votar por un determinado candidato, localiza el agujero con el símbolo que figura al lado del nombre del candidato y lo señala con un rotulador especial que facilita la lectura óptica. Esto en principio plantea un problema de usabilidad y accesibilidad importante. A través del agujero se ve la marca que corresponde a cada candidato. El elector marca su opción con el rotulador de punta gruesa que le ha facilitado la mesa y que necesariamente deposita tinta tanto en la parte superior del voto como en la inferior. Después separa ambas hojas y destruye la que la mesa le ha indicado, mediante una trituradora de papel delante de la mesa electoral, entregando el soporte con la hoja de la papeleta que ha quedado. Esta es leída con el equipo de escaneado óptico (OCR) que dispone la mesa y al mismo tiempo sale una copia por la impresora, que está conectada al mismo, y que será entregada a modo de recibo al votante, verificándose la coincidencia con el original que queda en la urna electoral. Cada par de papeletas tiene un número de serie único, que podría ser vinculado al votante pero no a su elección ya que la posición de los candidatos no es descubierta en ningún momento y se utilizará en el posterior proceso de verificación para asegurarnos de que el voto ha sido contabilizado. Este procedimiento para votar no es sencillo y así lo demuestra el hecho de que su utilización práctica en elecciones ha sido escasa y en entornos muy controlados, con un alto nivel de formación y un número reducido de votantes [163]. Además podría considerarse poco protegido con respecto a la anonimia por la fácil relación entre el número de serie y el votante.

El proceso de verificación es como sigue. El recibo del votante, es decir la copia de la mitad de la papeleta que se ha llevado, no indica cuál de los candidatos ha sido seleccionado por lo que se evitará la coacción sobre el votante. Después del recuento, la autoridad electoral publicará una imagen de cada recibo a través de una web. El votante puede buscar su voto escribiendo el número de serie y puede comprobar que la información en poder de la autoridad electoral coincide con su voto. De esta manera, el ciudadano puede estar seguro de que su voto fue tenido en cuenta como estaba previsto.

Cualquier elector o parte interesada puede también inspeccionar parte de los registros de los votos para verificar que los resultados se calculan correctamente, pero no pueden revisar toda la base de datos, ya que de lo contrario se podrían vincular votos a números de serie. Sin embargo, los autores aseguran que se puede inspeccionar la mitad de la base de datos sin romper el anonimato. Se demuestra con este procedimiento que la probabilidad de que todos los votos fueron contabilizados adecuadamente es muy alta [164].

4.2.1.4. Soporte criptográfico

En cuanto a la criptografía, se utilizan dos conceptos, la estrategia de compromiso y el protocolo de divide y elige. El primero trata de no revelar el secreto pero sí de demostrar que uno lo conoce. El segundo consiste en permitir que el auditor electoral pueda conocer una parte de la información de la votación para comprobar que los votos no han sido modificados pero garantizando la privacidad del votante.

El orden de los símbolos y de los nombres que aparecen en las papeletas son generados seudo-aleatoriamente para cada votación y por lo tanto difiere en cada una de ellas. Del mismo modo ocurre con el orden de los símbolos en los agujeros. Por esta razón, el recibo no contiene suficiente información como para determinar qué candidato fue elegido. Si se mantiene la capa superior, el orden de los símbolos a través de los agujeros es desconocido y si se mantiene la inferior, el orden de los símbolos al lado de los nombres de los candidatos también es desconocido. Por lo tanto el votante no puede demostrar a nadie cómo ha votado, lo que impide la compra de votos o la coacción a los votantes. Por otra parte a cada papeleta se le asigna un número de serie. La relación entre el número de serie y el tipo de papeleta solo se establece en el momento del recuento, mediante la introducción de las claves en poder de las autoridades electorales.

Es obvio que el sistema dispone de un algoritmo mediante el cual puede recuperar la información de la hoja que ha sido destruida, a partir del número de serie y con total seguridad.

Por las razones explicadas anteriormente no vamos a entrar en los detalles ya que los propios desarrolladores han integrado este proyecto en la siguiente propuesta (Scantegrity).

4.2.1.5. Análisis crítico

En este sistema, el Punchscan, al igual que en la mayor parte de los que vamos a comparar, subyace el predominio de la integridad por encima de la privacidad, ya que sin la primera es imposible detectar y evitar unas elecciones manipuladas, que son contrarias a la esencia democrática. A pesar de ello la privacidad es suficientemente robusta para garantizar el anonimato dentro de un margen aceptable, en función del tipo de votación.

En realidad los autores del sistema hablan de un sistema de votación basado en criptografía más que de un sistema de votación electrónica, ya que la seguridad de este sistema se fundamenta en su esencia matemática, más que en la habilidad del sistema en mantener los datos seguros.

La primera restricción es que no todos los tipos de votaciones son posibles con Punchscan, solo aquellas en las que tengamos que seleccionar una única opción entre varias, por lo que votaciones como las del Senado español serían imposibles. La segunda dificultad con la que cuenta este sistema es la relativa a los pasos previos a una votación, empezando por la impresión de las papeletas y la generación seudo-aleatoria de los números de serie, con las limitaciones que esto implica. También tenemos que calcular con acierto la cantidad de ellas que será necesario generar, ya que puede plantear problemas con la longitud de los números de serie que pueden crecer de forma desmesurada. Además está el aspecto del coste, la centralización y control del proceso de impresión (el que tenga acceso a él podría conocer la relación entre los números y el tipo de papeleta) y la distribución y custodia de las mismas. Ya ha quedado claro que el ciudadano no puede acceder de forma libre y sin control a las mismas, por lo que en algunos sistemas electorales no podría ser utilizado. Por otro lado está la gestión del hardware y software necesario en cada mesa, los procedimientos de puesta en marcha, votación, recuento y verificación por parte del votante y de las autoridades electorales. Esto nos lleva a la necesidad de una formación rigurosa y no precisamente sencilla del personal involucrado en el desarrollo de la votación y la no menos importante de los votantes.

Desde un punto de vista general podemos deducir que la mayor debilidad de este sistema, al igual que ocurre con otros similares, y que pone en peligro su integridad tiene que ver con la creación y lectura de estas complejas papeletas. Un diseño incorrecto, una

impresión errónea o una lectura defectuosa pueden poner en jaque todo el proceso. Esto sin tener en cuenta que el proceso de descifrado necesario para el recuento pueda tener problemas o sencillamente no funcionar. En estos casos sería necesario volver a repetir el proceso de votación.

Es evidente que las oportunidades de mejorar con la tecnología la usabilidad y la accesibilidad en el proceso electoral serían en este caso especialmente difíciles. Más bien lo contrario, complicarían el acceso al sistema tanto por la cantidad como por la complejidad de los pasos así como por el número de elementos que habría que utilizar: papeletas difíciles de interpretar, variedad de pasos intermedios, la utilización de un rotulador especial, destrucción de una parte de la papeleta, escaneo de la otra, verificación posterior en una pantalla, etc. Además, está la dependencia de un OCR para leer las papeletas y de una impresora que pueden presentar un sinfín de complicaciones a lo largo de una jornada electoral intensa.

Otra característica que habrá que regular sería la distribución de la información necesaria para realizar el recuento entre las autoridades electorales, que no debería confluir en ningún caso en una única persona por mesa, ni mucho menos a nivel general. No es esta una cuestión baladí, ya que por las características de su esencia criptográfica podría existir una persona o varias que controlaran y conocieran todos los detalles, pudiendo vulnerar desde dentro, la integridad o el secreto del proceso electoral. Esto es especialmente grave desde mi punto de vista.

En cuanto a los aspectos puramente criptográficos, no he podido profundizar debido a la falta de información clara y precisa al respecto. Si bien en principio parece ofrecer garantías suficientes, no deja de sorprender que a pesar de su corta vida y sus escasas pruebas, hayan aparecido diversos tipos de vulnerabilidades y posibles ataques al sistema, como ya hemos mencionado.

4.2.1.6. Conclusiones

Punchscan fue un sistema pionero de votación con verificación E2E aunque con documentación poco clara y detallada. El sistema se ha comportado como cabía esperar en todas aquellas pruebas en las que ha sido utilizado, que no han sido muchas, destacando como el mejor sistema de votación en el Vocomp del 2007 (claro que el "padre" del sistema también fue el creador de esta competición). El equipo que lo desarrolló ha sido capaz de innovar para cumplir con los requisitos que les impusieron en cada elección o prueba hasta el 2008. A partir del 2011 el sistema desapareció y con él el código abierto. En este momento este proyecto fue integrado en el sistema Scantegrity.

El aspecto más negativo de Punchscan es la complejidad del formato de votación ya que es desconocida para la mayoría de los votantes, por lo que sería necesaria una formación previa. La selección indirecta y aleatoria de la opción por parte de los votantes sobre la papeleta, puede suponer una fuente de problemas. El sistema de protección para impedir la votación incorrecta (voto nulo), es sin duda innovadora, pero supone un engorro en la práctica al ser difícil de explicar a los votantes. Sin embargo, este sistema ha supuesto sin duda un reconocido e importante esfuerzo innovador por parte del equipo desarrollador.

En cuanto al coste es evidente que depende del sistema con el que se compare: no es igual hacerlo con los sistemas clásicos que utilizan papel que con los apoyados en tecnología. Pero dentro de estos últimos, este no es especialmente oneroso ya que no requiere de sofisticados dispositivos, su software es abierto y no está sujeto a ningún tipo de pago por uso, aunque hay que tener en cuenta la cantidad de papel necesario debido a la doble papeleta utilizada.

La usabilidad presenta la dificultad de tener que seleccionar qué agujero marcar y para ello previamente hay que resolver cuál es el correcto. Por tanto es menos usable que una clásica papeleta en la que señalar nuestra elección, pero más sencillo que navegar entre las diversas pantallas de una DRE. Tampoco ayuda en este sentido la necesidad de una instrucción previa necesaria para poder utilizar este sistema. En cuanto a la accesibilidad, es cierto que este desarrollo se podría mejorar de forma evidente para los votantes con diversidades visuales o auditivas pero como reconocen sus desarrolladores no para ambas simultáneamente. Si la votación tiene pocos candidatos pudiera ser más vulnerable y con muchos sería más tedioso y lento para el votante.

En cuanto al aspecto de la administración del sistema es fácil concluir que no es sencilla y requiere de una preparación especial. Las autoridades electorales son responsables de una correcta puesta en marcha y gestión del proceso, y la multitud de pasos necesarios y su complejidad siembra de dificultades este aspecto del sistema. Es necesario configurar el sistema, gestionar la producción de papeletas, generar las firmas y códigos de acceso, resolver las impugnaciones si aparecen, lo que nos obligaría a conocer el sistema con detalle y como ha quedado evidenciado esto no es sencillo.

Punchscan está bien diseñado para prevenir algunos ataques y errores no maliciosos. En primer lugar los errores en la generación de las papeletas serían detectados en la comprobación previa. Según los autores, si durante el proceso electoral fallara algún dispositivo electrónico, las elecciones podrían continuar si se toman los datos de forma manual y reteniendo la parte de la papeleta que habría que destruir, pero esto complicaría aún más el proceso y añadiría riesgos al secreto del voto, convirtiéndolo en una chapuza.

La integridad y verificabilidad de los resultados es el aspecto más fuerte de este sistema como hemos descrito anteriormente. Es muy importante la posibilidad de comprobar el código de la aplicación al ser abierto y las primitivas de seguridad empleadas para proteger la información son consideradas hoy en día suficientemente robustas (AES y SHA-256) aunque mejorables. La privacidad no está suficientemente protegida ya que, aunque en ningún caso el sistema de reconocimiento óptico de los votos explora toda la papeleta, la información para realizar el recuento posterior está en manos de los miembros de la mesa electoral. Es por ello que en los trabajos indicados se habla de privacidad pero no de secreto en el proceso.

El sistema cumple en lo esencial con las comprobaciones posibles, tanto la que puede llevar a cabo el elector para comprobar que su voto ha sido tenido en cuenta de la misma forma en que fue emitido y la general que pueden llevar a cabo las autoridades electorales.

4.2.2. Scantegrity

4.2.2.1. Origen

Es una variante evolucionada de la anterior propuesta por el mismo autor, David Chaum, con la colaboración de otros investigadores como Ronald Rivest y Peter Ryan [63] [59]. El proyecto ha sido mejorado por propuestas de los mismos autores, como el Scantegrity II [147], o por terceros como el caso del Scantegrity III [165].

Nuestro análisis principal se basa en la versión II por ser la más documentada. Destaca por haber sido utilizada en varias pruebas y procesos electorales [166] desde el 2007 al 2011 [167].

Esta solución es sin duda una de las más estudiadas de todas las propuestas, ya que incluso se desarrolló una tesis doctoral por Richard Carback en 2010 con un análisis muy completo y profundo [143].

Esta propuesta ha sido utilizada en diversas ocasiones lo que ha conseguido mejorar y refinar su diseño. La primera ocasión fue el 9 de noviembre de 2007 en la conferencia "Claim Democracy" en su versión inicial. Posteriormente, en 2008, las experiencias se desarrollaron con Scantegrity II en diversas consultas populares en Ottawa (grupo de usuarios de Linux) y en Takoma Park [166]. La más singular e importante se desarrolló el 3 de noviembre de 2009 [165] en las elecciones municipales de esta última localidad americana. A raíz de esta votación se propusieron diversas mejoras que concluyeron con la propuesta del Scantegrity III, pero que no ha llegado a ser utilizada en ningún proceso electoral.

4.2.2.2. Características

En este caso la votación se realiza mediante una lectura óptica de la papeleta mediante un OCR y manteniendo al mismo tiempo las papeletas originales para que puedan ser analizadas de nuevo manualmente si fuera necesario. A diferencia del caso anterior, este sistema puede ser utilizado en cualquier proceso que utilice un escáner óptico convencional y se desarrolla como un proceso de votación muy similar al clásico, en el que no hay que añadir ningún equipamiento adicional, salvo una impresora para imprimir información adicional sobre la papeleta en el momento de la impresión. Está claro que, como el votante se queda con una parte de la papeleta original que puede relacionarse directamente con el voto emitido, puede suponer un riesgo importante el hecho de poder acceder a las papeletas depositadas en la urna en el momento del recuento. En la segunda variante, Scantegrity II, se utiliza papel especial que oculta códigos de confirmación de la selección que sólo son visibles cuando son marcados con una tinta especial, lo que sin duda complica el proceso de impresión y lo encarece, pero mejora el principal inconveniente de la anterior versión que era la resolución de las impugnaciones. Todos estos aspectos los veremos con detalle a continuación y el resto son muy similares al Punchscan.

Sobre la base del Punchscan, es decir sobre un sistema de votación basado en el escaneo óptico del voto, se optó por integrar un proceso seguro de verificación, lo que obligó a un diseño nuevo y específico de la papeleta y a modificar el procedimiento de votación. En principio el Scantegrity sólo necesita que se imprima en las papeletas una información adicional que no aparecía en el Punchscan, pero, como veremos, eso plantea nuevos problemas. Como quiera que las papeletas son únicas, es esencial desligar la papeleta del votante. Para ello se utiliza la sencilla solución de dividir la papeleta en dos en el momento de depositar el voto, no existiendo mecanismo que pueda unirlas salvo bajo la supervisión de las autoridades electorales y sólo para el recuento. Claro está que para que los electores tengan confianza en la capacidad de la solución para hacer un recuento fiable, determinada información ha de ser publicada para poder realizar la verificación.

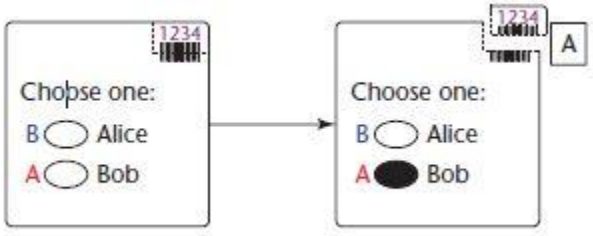
En esta solución, al igual que en otras, parte de los votos, típicamente la mitad, son elegidos al azar antes de las elecciones para realizar una verificación pública y demostrar que la propuesta es fiable. Lo más complejo es revelar la suficiente información para verificar el voto sin comprometer el secreto del mismo. Otro aspecto delicado es resolver las impugnaciones entre el votante y las autoridades electorales cuando el primero asegure que su voto no ha sido contabilizado correctamente.

4.2.2.2.1 Procedimiento de votación con Scantegrity

En la primera versión del Scantegrity el procedimiento era similar al utilizado en cualquier votación con escáner óptico, en el que el elector deposita la papeleta en la urna que es leída por el OCR, salvo que el votante se llevaba a casa un recibo de su voto. Por tanto éste recogía la papeleta, en la que la relación entre los candidatos y las letras que tiene que marcar el votante no son únicas, y señala con un rotulador especial su elección para a continuación entregar su voto en la urna con lectura óptica. La única diferencia que aprecia el votante con respecto al voto clásico en urna con lector óptico, es que puede arrancar parte de la papeleta que contiene un número de serie y su codificación en código de barras y en la que puede anotar la letra asociada al candidato elegido. Después del recuento se publican los números de serie y la letra asociada a cada uno de ellos sin desvelar el nombre del candidato. De esta forma el elector puede verificar que su voto ha sido correctamente explorado y registrado pero no puede demostrar a un tercero a quién votó. El problema aparece cuando el votante discrepa de la opción por la que ha votado y desafía al sistema impugnando la votación.

En este caso el procedimiento para resolver la impugnación tiene dos pasos que de alguna forma ponen el peligro la privacidad del voto. En primer lugar los miembros de la mesa tienen que recuperar la papeleta original leída por el escáner óptico para verificar el número de serie pero no su contenido, algo que evidentemente ha de hacerse con las suficientes garantías. En segundo lugar ha de comprobarse la opción marcada sin comprometer al candidato seleccionado leyendo el número de serie y buscando la coincidencia con el listado publicado después del recuento. Si esta no se produce, es suficiente para que la impugnación prospere y se modifique el recuento. Todo esto evidenció la débil estructura de resolución de conflictos y propició la aparición del Scantegrity II (Invisible Ink), que es el modelo que en realidad vamos a estudiar.

Ilustración 12. Papeleta del Scantegrity I [59].



4.2.2.2.2. Procedimiento de votación con Scantegrity II

Esta versión proporciona una mayor inmunidad a la coerción sobre el votante puesto que no existe relación directa entre el número de serie de la papeleta utilizada y la posición de las marcas sobre la misma, ya que esto se resuelve utilizando unos rotuladores que descubren, mediante tinta especial, unos números ocultos que además permiten la resolución de impugnaciones de una forma que los autores defienden como más sencilla y transparente.

El procedimiento de votación con Scantegrity II es muy similar al de un sistema de votación con escáner óptico, excepto que la casilla en la que se señala la elección contiene un código de confirmación impreso al azar y en tinta invisible. El votante marca la casilla elegida con un bolígrafo "decodificador" diseñado al efecto, que activa la tinta invisible provocando que aparezca un código de confirmación. Esta es una diferencia esencial con la primera versión, que repercute en el procedimiento para la impugnación del voto ya

que en la primera versión el proceso era complejo e implicaba a las autoridades electorales.

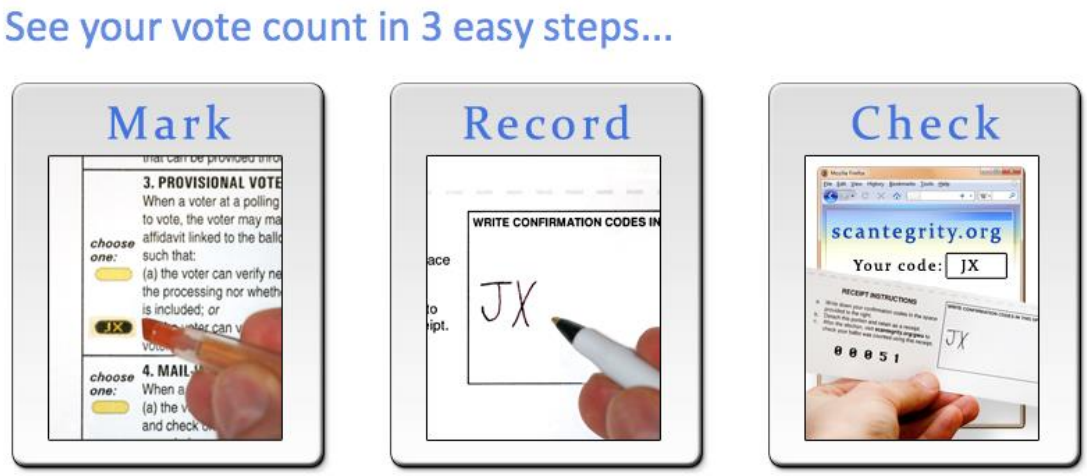


Ilustración 13. Detalle de la votación con la papeleta Scantegrity II (scantegrity.org).

.

Los electores que deseen comprobar su voto posteriormente pueden anotar los códigos de confirmación en un cupón recortable que contiene el número de serie de la papeleta, o bien pueden sencillamente ignorar el código y emitir su voto con normalidad. Sin duda esto simplifica el problema de diseño, a pesar de mantener la dependencia de unas impresoras especiales y de unos escáneres ópticos fiables. En cualquier caso es una debilidad ya que puede verse afectado por errores de impresión y de anotación por parte del votante.

Los códigos de confirmación se asignan aleatoriamente en las papeletas de voto por lo que los votantes pueden compartir libremente sus códigos manteniendo en secreto su voto, aunque no le conste fehacientemente que su código corresponda a su elección en el momento del recuento.

Una vez finalizada la votación, la autoridad electoral publica una lista con los códigos de confirmación seleccionados en cada papeleta sin precisar la posición, con lo que no se compromete el secreto del voto y se evita la coacción. Los votantes que copiaron sus códigos pueden verificar que se han tenido en cuenta en el escrutinio y que no se han quitado ni añadido otras opciones. Los autores demuestran que la probabilidad de adivinar al azar un código que haya aparecido en una papeleta electoral es muy baja.

Después del recuento, los administradores electorales generan una lista por número de serie con las papeletas y sus códigos de confirmación. Dado que el vínculo entre el código de confirmación y el candidato votado permanece en secreto, el recuento se realiza utilizando un proceso que garantiza la preservación del anonimato. El recuento puede ser comprobado por cualquiera para asegurar su precisión (verificación universal).

La seguridad del sistema no requiere de ningún software específico para funcionar correctamente, sólo necesita que las operaciones matemáticas (que no son públicas) sean confirmadas de forma independiente por todas las partes interesadas, sobre todo en lo que se refiere a la generación aleatoria de los números de serie de las papeletas y a los códigos de elección.

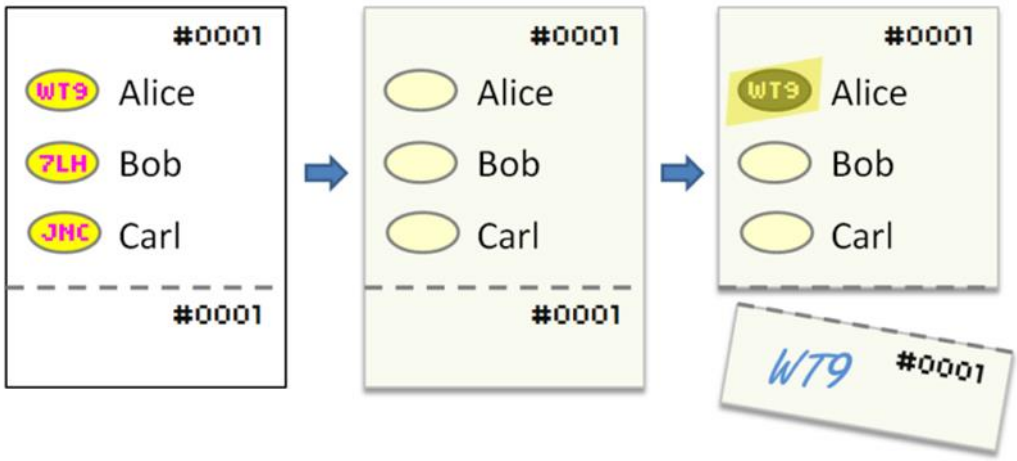


Ilustración 14. Detalle del proceso de votación con Scantegrity II [147].

El Scantegrity II mejora la integridad del sistema original dado que evita la coerción directa aun disponiendo de acceso a las papeletas ya que los códigos están ocultos y la única forma de acceder a ellos es invalidar la votación. Obviamente la parte de la papeleta depositada en la urna contiene ambas informaciones, es decir el número de serie y el código con la elección, por lo que el acceso a las mismas está restringido a los miembros de la mesa y sólo si fuera necesario acceder a ellas.
Ahora bien, las papeletas y su validez dependen de procesos químicos que pueden fallar o ser alterados por otros, lo cual puede poner en peligro todo el proceso electoral. Para la impresión de las papeletas se utilizan tres tipos de tintas diferentes: una es tinta convencional para la impresión de los datos básicos de la votación más los nombres de los candidatos; las otras dos tienen que ver con los códigos de confirmación y con el sistema de lectura óptico. Las interacciones entre éstas y el producto químico que las activa, presente en el rotulador utilizado para marcar el voto, no son sencillas y constituyen una fuente de problemas adicionales en este tipo de sistemas.

Las pruebas reales realizadas con este sistema, como veremos en el apartado correspondiente, dejaron patente que algunos votantes no escribían los códigos de verificación para poder posteriormente realizar la comprobación sobre su voto y que el votante no era informado con claridad de cuántas opciones disponía al votar por lo que podía hacerlo de forma incorrecta.

4.2.2.2.3. Procedimiento de votación con Scantegrity III

En esta tercera variante, propuesta por Sherman et al. [165] se definen mejoras obtenidas mediante observación en una elección real en noviembre del 2009 [165]. La más destacada se refiere a la impresión automática del recibo de verificación, lo que reduce la instrucción previa del votante y por tanto mejora la usabilidad, incrementa la accesibilidad, facilita la detección por parte del votante de la manipulación de su voto y hace más sencilla la verificación posterior. En cambio la aparición de las impresoras necesarias puede comprometer la privacidad del voto.

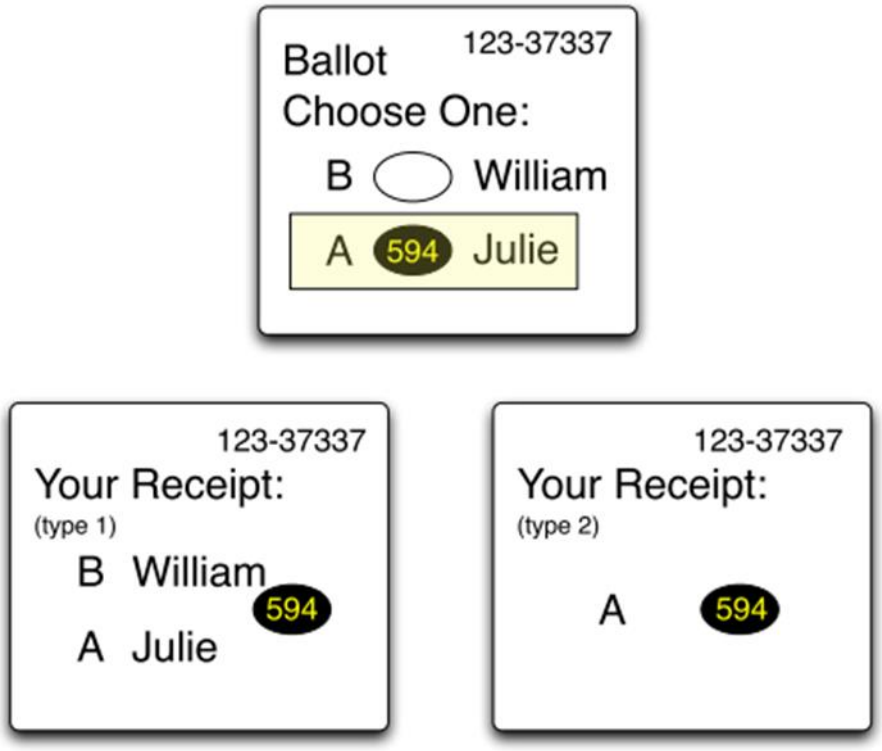


Ilustración 15. Variante mejorada de la papeleta del Scantegrity III [165].

Lo que se intenta en esta versión es generar el recibo de verificación de forma automática y más cómoda. Una vez que la papeleta es marcada por el votante, se coloca debajo de una tapa de cristal donde es explorada ópticamente y los detalles más importantes, letra, nombre y código de la opción elegida, son destacados con una luz trasera. Posteriormente se visualizan los dos formatos disponibles de recibo de verificación para de forma aleatoria imprimir uno de ellos. Este mecanismo de impresión reduce los riesgos en esta parte del proceso. Esto permite simplificar el proceso y mejorar aspectos como la notificación al usuario de haber rellenado correctamente la papeleta y reducir la posibilidad de que la misma sea modificada posteriormente añadiendo marcas después de contabilizada, que podrían llevar a la impugnación del proceso.

Como acabamos de explicar, esta versión intenta aumentar la usabilidad del sistema mediante la retro-iluminación de la papeleta en el momento de la lectura óptica, destacando los aspectos básicos del voto. Para cumplir con estos aspectos aparece un nuevo dispositivo, denominado PCOS, que integra el escáner óptico con retro-iluminación, el detector de las marcas en las papeletas y la impresora que entrega el recibo de votación en uno de los dos formatos definidos. Los objetivos se han descrito anteriormente, pero su diseño exclusivo y la explicación necesaria para justificar que elimina la necesidad de la verificación en el proceso de impresión del recibo, complica el desarrollo y seguimiento del proceso electoral con esta versión. Sería muy importante realizar más pruebas piloto con el objeto de comprobar lo que los autores sostienen en cuanto a ventajas en comodidad, rapidez y accesibilidad.

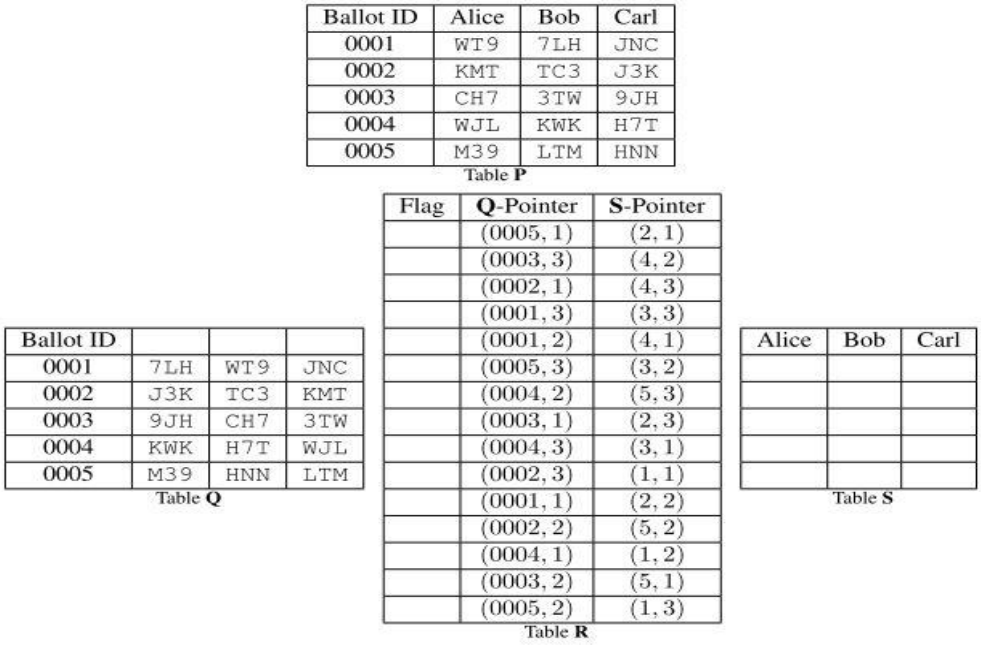
4.2.2.3. Soporte criptográfico

Este sistema utiliza un generador de números seudo-aleatorios (PRNG) como en el caso anterior pero utiliza cuatro tablas para realizar las operaciones de mezcla (mixnets). Estas tablas se denominan P, Q, R y S. La tabla P relaciona los códigos de confirmación y los candidatos en cada papeleta, se genera bajo la supervisión de las autoridades electorales y nadie debería de tener acceso a ella, pero se utiliza para generar la tabla Q. En ésta se publican los códigos de confirmación pero realizando una permutación seudo-aleatoria de forma que cada fila i corresponda a la papeleta i pero en cada columna no hay correspondencia con candidatos fijos. De esta tabla Q sólo se publican los códigos de confirmación utilizados. En la tabla R se desarrollan dos mezclas al azar de los códigos de confirmación y será utilizada en el procedimiento de comprobación y está unida a la tabla anterior por un puntero. En la tabla S, que se hace pública al final del recuento, cada elemento es un código de confirmación que ha sido utilizado en la votación pero no se muestra su relación con el candidato votado.

Toda esta red de mezclas permite aislar una determinada papeleta de la opción marcada a la vez que permite el recuento correcto bajo la supervisión de la autoridad electoral que posee las claves para activar el proceso de recuento automatizado, en el momento determinado y sin desvelar la privacidad del voto. Para resolver una impugnación planteada por el votante, éste ha de proporcionar el número que identifica su papeleta y el código de confirmación. Posteriormente la mesa verifica la relación entre ambos sin desvelar el sentido del voto.

En la ilustración 16 se observa que el voto por Alice en la papeleta identificada como 0001 corresponde al código de verificación WT9, según la tabla P. El mencionado código está en la tabla Q en la fila 1 y columna 2 (0001,2). Este puntero se corresponde con el (4,1) mediante consulta de la tabla R. Por último la tabla S nos indica que en esa posición el voto corresponde a Alice (fila 4 y columna 1). Estas tablas son generadas por las autoridades electorales para resolver el recuento pero no son publicadas nunca y sólo ellos tienen acceso a las mismas de una forma mancomunada.

En la ilustración 17 aparecen las tablas que se publican para resolver la verificación por parte del votante. En ningún caso se publica la tabla P. Tampoco se descubre toda la información del resto de las tablas. La información es suficiente para relacionar el código de verificación (en nuestro caso WT9) con uno de los *flags* presentes en la tabla S sin especificar la posición y sólo de aquellas papeletas que han sido utilizadas (en nuestro caso, cuatro), permitiendo establecer con seguridad el resultado: 2 votos para Alice, 1 para Bob y 1 para Carl.



Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Table **P**

Flag	**Q**-Pointer	**S**-Pointer
	(0005, 1)	(2, 1)
	(0003, 3)	(4, 2)
	(0002, 1)	(4, 3)
	(0001, 3)	(3, 3)
	(0001, 2)	(4, 1)
	(0005, 3)	(3, 2)
	(0004, 2)	(5, 3)
	(0003, 1)	(2, 3)
	(0004, 3)	(3, 1)
	(0002, 3)	(1, 1)
	(0001, 1)	(2, 2)
	(0002, 2)	(5, 2)
	(0004, 1)	(1, 2)
	(0003, 2)	(5, 1)
	(0005, 2)	(1, 3)

Table **R**

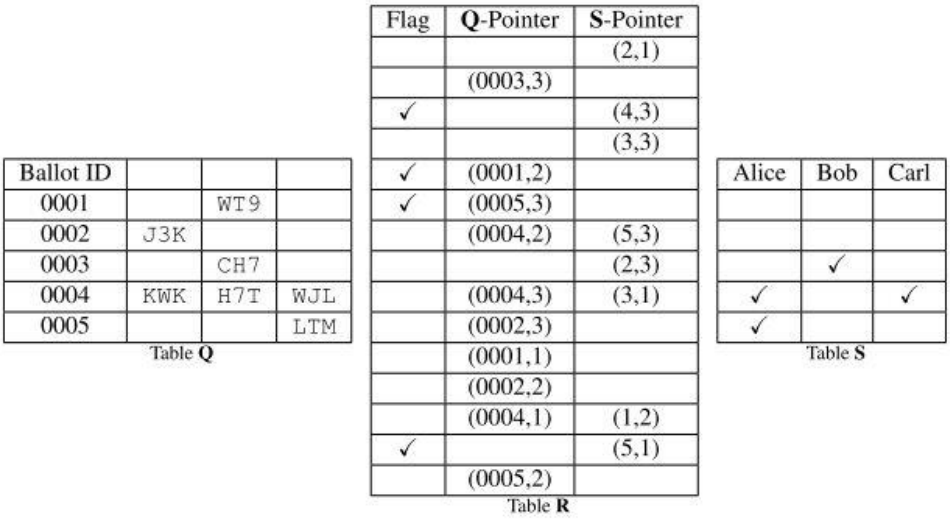
Ballot ID			
0001	7LH	WT9	JNC
0002	J3K	TC3	KMT
0003	9JH	CH7	3TW
0004	KWK	H7T	WJL
0005	M39	HNN	LTM

Table **Q**

Alice	Bob	Carl

Table **S**

Ilustración 16. Tablas P, Q, R y S (generadas antes de las elecciones con Scantegrity II) [147].



Flag	**Q**-Pointer	**S**-Pointer
		(2,1)
	(0003,3)	
✓		(4,3)
		(3,3)
✓	(0001,2)	
✓	(0005,3)	
	(0004,2)	(5,3)
		(2,3)
	(0004,3)	(3,1)
	(0002,3)	
	(0001,1)	
	(0002,2)	
	(0004,1)	(1,2)
✓		(5,1)
	(0005,2)	

Table **R**

Ballot ID			
0001		WT9	
0002	J3K		
0003		CH7	
0004	KWK	H7T	WJL
0005			LTM

Table **Q**

Alice	Bob	Carl
	✓	
✓		✓
✓		

Table **S**

Ilustración 17. Tablas Q, R y S (publicadas después de las elecciones con Scantegrity II) [147].

4.2.2.4. Análisis crítico

En principio esta propuesta permite utilizar unas papeletas de votación parecidas a las habituales y equipos con escáner óptico, por lo que el votante no debería sorprenderse. La sorpresa puede surgir al ver que los recibos para la verificación posterior no son generados de forma automática (en las versiones inicial y II) y obliga al votante a tomar nota de los códigos.

Como en casi todos los casos aquí estudiados, esta solución permite tanto a los votantes de forma individual como a las autoridades electorales y a los interventores u observadores externos, verificar que las papeletas han sido tenidas en cuenta de forma correcta.

Las debilidades que presenta esta solución son las relativas a la accesibilidad de las papeletas y su dependencia del proceso químico relacionado con la impresión y visualización de los códigos de elección, además del coste de la impresión de las papeletas y del equipamiento utilizado, como el escáner óptico y la impresora. Por otro lado están los problemas que pueden suscitarse con el votante en cuanto a desacuerdos (repudio) de su selección, ya que depende de la anotación a mano que realiza del código que, por error o mala fe, puede diferir del visualizado en la página de verificación publicada. Este aspecto es solucionado en la versión III.

También pueden aparecer posibles ataques a la integridad del método si se conocen los números de serie y los códigos ocultos relacionados de cada papeleta, aspecto este que en cualquier caso puede estar al alcance de las autoridades electorales. La posibilidad de acceder antes de la votación a las papeletas puede dar lugar a un sinnúmero de manipulaciones y ataques que podrían complicar los procesos de lectura de las papeletas, de verificación y de resolución de conflictos. Por otro lado en elecciones con un gran número de elegibles puede complicar sobremanera el diseño de las papeletas y del procedimiento que se debe seguir.

Sigue siendo posible que alguna de las personas implicadas en la gestión electoral tenga acceso a las papeletas antes de las elecciones y pueda coaccionar a los votantes mediante la comprobación del recibo. Por mucho que se proteja el mecanismo de votación con recibo, éste siempre será un riesgo. En este sentido y sin tener acceso previo a las papeletas, se puede forzar a votar siempre a la misma posición, creando una votación al azar, que beneficiaría a los más votados.

En la segunda versión del Scantegrity y al contrario que en el original, la resolución de conflictos no se basa esencialmente en el recibo de papel con el que se queda el votante, ni requiere que los funcionarios electorales realicen operaciones complejas y delicadas. Además Scantegrity II aunque mantiene la identificación de la papeleta mediante un número único, añade una información exclusiva que recibe el votante en la cabina de votación y que puede o no anotar a mano en la papeleta para evitar coacciones posteriores, obteniendo de esta forma un importante incremento de la privacidad.

Otro aspecto delicado es el crítico proceso químico de tintas en la versión II que obligaría la presencia de expertos en este tipo de impresiones en el proceso electoral para resolver problemas como la desaparición de las marcas o el funcionamiento erróneo del mecanismo por problemas de temperatura, humedad o contacto con líquidos extraños. Algunos autores [140] [143] proponen evitar el uso de estas tintas e integrar los códigos de verificación utilizando plataformas seguras, pero este aspecto no ha sido desarrollado todavía.

A partir de la versión II sí se mejoran la usabilidad, la resolución de impugnaciones y la mejora contra la coacción. En cambio el proceso de impresión del recibo complica la votación y aumenta el coste de su puesta en marcha. La ventaja de esta versión es que no es necesario recuperar la papeleta para resolver las impugnaciones.

4.2.2.5. Conclusiones

Tras el análisis realizado, cabe pensar que existen tres razones evidentes para ser escépticos en cuanto a las perspectivas del Scantegrity. En primer lugar, el sistema no es precisamente un modelo de simplicidad, ya que sólo la explicación básica del sistema

lleva su tiempo. En segundo lugar, los funcionarios electorales se inclinan por simplificar los procesos electorales especialmente si se utilizan estas tecnologías: un sistema que combina la criptografía y la web debería ser más simple y accesible. En tercer lugar, es necesaria la presencia de mecanismos de verificación que permitan al ciudadano y a las autoridades comprobar la fiabilidad del sistema. Es evidente que en ningún caso vamos a obtener unas garantías plenas, pero lo que no debe la tecnología es incrementar los recelos del votante. Y como la historia de la tecnología deja muy claro, en un concurso entre lo perfecto pero complicado y lo suficientemente bueno pero sencillo, gana este último.

La opción de la última versión, Scantegrity III, de incorporar un dispositivo de lectura de marcas e integrarlo en una plataforma segura, evitando tener que escribir los códigos de verificación, puede ser un avance importante ya que evitaría el delicado aspecto de la química de las tintas invisibles y simplificaría el proceso, aumentando la usabilidad. Pero a día de hoy sólo es una propuesta teórica.

En cualquier caso estas propuestas confieren una mayor integridad al proceso electoral, rapidez en el recuento y verificabilidad del sistema que los sistemas basados en VVPAT, pero quedan pendientes problemas de implementación, de usabilidad y accesibilidad.

El delicado equilibrio entre la posibilidad de que el votante se lleve a casa un recibo para verificar su voto y por otro, los riesgos de pérdida de la privacidad y falsas denuncias de irregularidades, debe ser el principal objetivo que persigan estas propuestas, objetivo harto complicado como está quedando de manifiesto.

4.2.3. Threeballot

4.2.3.1 Origen

ThreeBallot es un protocolo de votación desarrollado en el 2006 por Ronald Rivest [148]. Es un sistema que puede ser implementado en papel convencional. El objetivo de su desarrollo es obtener un diseño sencillo, de fácil comprensión y que no utilice técnicas de cifrado complejas. Es curioso resaltar que sea precisamente este autor, reconocido experto en criptografía, el que proponga un método con un bajo nivel de uso de la misma. Todo ello con el ánimo de que de forma simultánea el voto sea verificable y anónimo.

Ha sido utilizado en una votación en diciembre de 2006 por estudiantes del M.I.T. que dejaron patente problemas de privacidad, seguridad y usabilidad. [168]. En ella el 20% de los votantes consiguieron vender sus votos, el 10% no fue capaz de verificarlo y el 30% no consiguió emitir correctamente el voto en el primer intento.

4.2.3.2 Características

ThreeBallot intenta resolver el problema de la contraposición entre verificabilidad y anonimato dando a cada votante tres papeletas. De una de ellas se hará una copia y servirá de recibo y las tres se depositarán por separado en la urna. Cada papeleta de las tres tiene un número único y distinto, intentando evitar que el número sea excesivamente grande con objeto de que sea más sencilla su gestión. El votante elige qué papeleta va a ser su recibo para verificar la votación. El que recuenta los votos obviamente no lo sabe y tiene una probabilidad de 1/3 de ser descubierto destruyendo o alterando el voto. El elector vota por una opción (sí/no) o candidato en cada fila de forma que está obligado a marcar un par de veces para que sea válida, ya que una marca no es suficiente por razones que veremos a continuación. De esta forma el recuento sólo es válido si tiene dos marcas

en cada fila, que corresponden a un candidato o pregunta. Por ello para votar por un candidato el elector debe seleccionarlo en dos de las tres partes de la papeleta.

Para votar en contra de un candidato (el equivalente a dejar un voto en blanco en otros sistemas), el votante debe seleccionar a ese candidato solamente en una papeleta. Ningún candidato puede dejarse en blanco, ni se puede seleccionar en las tres papeletas. Este aspecto es una debilidad del sistema, pues tiene que ser verificado antes del depósito de las tres papeletas mediante algún tipo de lector mecánico u óptico, con objeto de evitar los votos nulos (en este sistema no se admiten). El recibo con el que se queda el votante, es decir una copia de una de las tres partes de la papeleta, no puede demostrar a un tercero a quién se ha votado, con lo que se evita la compra de votos y la coacción sobre el votante. Todos los votos emitidos son escaneados y publicados después del recuento para proporcionar un procedimiento de verificación y para detectar manipulaciones en los votos depositados. Es imposible relacionar las tres partes de la papeleta y sus números de serie son aleatorios y únicos. La criptografía necesaria es de muy bajo nivel y por tanto el sistema es fácil de explicar y de implementar.

BALLOT	BALLOT	BALLOT
President	President	President
Alex Jones ○	Alex Jones ○	Alex Jones ○
Bob Smith ○	Bob Smith ○	Bob Smith ○
Carol Wu ○	Carol Wu ○	Carol Wu ○
Senator	Senator	Senator
Dave Yip ○	Dave Yip ○	Dave Yip ○
Ed Zinn ○	Ed Zinn ○	Ed Zinn ○
3147524	7523416	5530219

Ilustración 18. Papeleta de ThreeBallot [148].

4.2.3.3 Procedimiento de votación

En primer lugar el votante selecciona aleatoriamente una de estas papeletas triples. A continuación marca su elección por filas de tal forma que no puede dejar ninguna fila en blanco y al menos ha de poner una marca por fila, ya que de otra forma el voto no será válido y detectado como tal en el momento de la emisión. Si el votante desea NO VOTAR por un determinado candidato tiene que realizar UNA marca en la fila correspondiente en cualquier posición (columna). Esto sin duda plantea problemas de usabilidad del sistema. Si el votante desea VOTAR a favor de un candidato necesita poner DOS marcas en esa fila y en cualquiera de las tres columnas de la papeleta. En ningún caso debe marcar TRES ya que el voto también sería nulo y no sería admitido en la urna.

Antes de depositar la papeleta es necesario verificar la validez del voto y esto tiene que realizarse en un equipo que explore ópticamente el voto y detecte los nulos impidiendo la emisión del mismo. Obviamente este sistema no puede estar conectado a nada ni tener capacidad de almacenar información, lo cual puede no resultar obvio.

Una vez verificada la validez de la papeleta, el proceso de votación se desarrollará de la siguiente forma: se procederá a separar las tres partes de la papeleta en presencia de la mesa pero sin mostrar las opciones marcadas, se realizará la copia en privado pero bajo

la supervisión de los miembros de la mesa, de una de las tres partes de la papeleta que el votante elegirá libremente y que mantendrá como recibo para la verificación posterior y por último, las tres papeletas originales se dejan caer en la urna por separado. La copia que ha de ser realizada bajo la supervisión de los miembros de la mesa es para evitar que el votante haga una copia de toda la papeleta. Por supuesto, una debilidad que aparece en este momento es la posibilidad de capturar una imagen de la papeleta completa para demostrar a terceros el voto emitido.

Al final de la votación todas las papeletas se publican, mediante un sitio web que hará las veces de tablón de anuncios y en el que cada elector puede verificar que sus votos fueron contabilizados buscando el número de su recibo (copia de papeleta elegida) entre los números de las papeletas publicadas. Sin embargo, con el recibo del elector no se puede deducir cuál ha sido su voto válido ya que ha podido quedarse con cualquiera de las papeletas, por lo que no puede demostrar a un tercero el sentido de su voto eliminando la posibilidad de coacción. También existe la posibilidad de impugnar la votación en el caso de que el recibo no aparezca o no coincida con el publicado, lo que podría poner en jaque todo el proceso electoral. Si el número de triples papeletas contabilizadas coincide con el número de votos emitidos podemos estar seguros que no se han añadido durante el proceso.

El principio clave de este sistema se basa en considerar cada voto como una matriz, en la que las filas corresponden a cada candidato o pregunta y en las que el votante se debe fijar para expresar su elección (votar por filas), pero el procesamiento del voto se hace depositando en la urna las tres partes de la papeleta por separado, siendo recontadas por el sistema (procesado por columnas).

Si la papeleta está correctamente diseñada, disponiendo dos líneas micro-perforadas que permitan la separación limpia de las tres partes, una zona para marcar la opciones diseñada para permitir la lectura automatizada por parte de un escáner óptico y los números de serie de cada una de las tres partes de la misma impreso en código de barras, posibilitaría una lectura simple y rápida de cada voto. Con ello sería rápido y fiable el recuento y la publicación de todos los votos.

En cuanto al recuento es más sencillo de lo que parece. En realidad cada candidato o pregunta tiene de partida un voto por cada votante ya que al menos una de las tres papeletas ha de ser marcada. Pero adicionalmente aquellas que han sido seleccionadas por el votante han recibido una marca más, que es la que realmente tiene que contabilizarse. Por ejemplo, si las personas que han votado son n y los candidatos tres, A, B, C y en el recuento final han recibido respectivamente x, y, z votos, el resultado final real será calculado restando n de los votos contabilizados. De esta forma el candidato A habrá recibido x-n votos y así respectivamente.

4.2.3.4 Soporte criptográfico

La usabilidad de esta solución es alta si se desarrolla una formación básica inicial para evitar errores. Es sencillo ya que el procedimiento se basa en marcar una vez para votar en contra y dos para votar a favor, pero evidentemente no es lo habitual. Además hay que dejar claro que no se puede dejar en blanco, ni marcar tres veces por opción (aspecto que es verificado antes de depositar el voto).

Otro aspecto destacado es que el sistema es tan seguro como otros basados en criptografía de alto nivel, pero sin utilizar ninguna de estas técnicas. También tiene un alto nivel pedagógico para explicar el valor que tiene la posibilidad de una verificación posterior del voto.

Es evidente que el sistema se basa en que la autoridad electoral tiene que disponer de los números de serie de las tres papeletas que integran cada voto para poder imprimir las papeletas y resolver las impugnaciones. El aspecto más crítico es que el proceso de impresión de las papeletas tiene que ser muy controlado. Por supuesto se podría combinar con un uso parcial o total de un equipo DRE, ya sea para imprimir el voto una vez emitido o incluso para almacenarlo y contabilizarlo.

Esta propuesta es fácil de explicar, tiene un bajo nivel de complicación matemática en el diseño y proporciona un buen nivel de verificabilidad global. Ahora bien, el hecho de utilizar votos en papel crea una serie de debilidades similares a los sistemas basados en VVPAT y volvemos a encontrarnos con diversas posibilidades de ataques ya comentadas y con otras nuevas que analizaremos a continuación.

4.2.3.5 Análisis crítico

Para empezar existe un estudio profundo y claro sobre esta propuesta en el que se ponen en evidencia sus riesgos y limitaciones [169].

Para garantizar el anonimato es importante que este esquema impida reconstruir la papeleta una vez separadas las tres partes, a pesar de la publicación de todas las hojas al final del recuento, con el fin de evitar la compra de votos o la coacción sobre el votante y mantener el secreto del voto. Por desgracia es posible vincular las papeletas que constituyen una unidad de varias maneras, por ejemplo, recordando los identificadores de las mismas, marcando las papeletas siguiendo un patrón definido y fácilmente reconocible cuando las papeletas se publican para su verificación ("ataque italiano"), añadiendo señales identificables en las papeletas, apuntando los números de identificación o sencillamente fotografiando las mismas. Para evitar el mencionado "ataque italiano" se pueden imprimir las papeletas de forma que esté pre-impresa una marca en cada fila de forma aleatoria, lo que sin duda complica un poco más la impresión de las mismas y la formación del votante (usabilidad).

Otro aspecto presente en todas las votaciones en las que se tiene acceso físico a la papeleta, es el riego del denominado voto en cadena, que se inicia cuando se consigue tener acceso a las papeletas antes de la votación. De esta forma se accede a la cabina de votación con la papeleta marcada bajo la supervisión de un tercero y se regresa con otra en blanco que será utilizada por el siguiente votante de la cadena. Para evitarlo habría que detectar que la papeleta emitida es la misma que le entrega al votante la mesa en el momento de la votación o impidiendo el acceso a los votos antes de la apertura de la mesa ya que podría comprometer el secreto. En otras palabras, el mero hecho de dividir una papeleta en tres partes proporciona una serie de vulnerabilidades propias de trileros.

En estos casos, al igual que en su momento veremos con la solución Prêt à Voter, el proceso de impresión de las papeletas ha de ser verificado para evitar que aparezcan repetidos los números de serie, ya que de esta forma podríamos conocer lo que ha votado un ciudadano mediante el recibo de verificación y la información publicada después del recuento.

Por otro lado el sistema tiene que ser muy escrupuloso con la introducción de todas las papeletas que constituyen el voto, ni más ni menos, e impedir cualquier cambio en las marcas, ya que cualquier alteración podría poner en entredicho todos los votos depositados en la urna. Como en cualquier otro caso la manipulación incorrecta o adrede por parte de los funcionarios electorales comprometería el resultado y la verificación del proceso. Además también pueden aparecer ataques de denegación de servicio contra la web en la que se publican los datos.

Una contramedida para evitar recordar o apuntar el número que identifica el voto es utilizar algún tipo de código de barra, aunque también hace la verificación más compleja. Otro aspecto importante es que el equipo necesario para verificar que el voto ha sido emitido correctamente debería ser una máquina que no permitiera almacenar información de la lectura y que sencillamente verifique si la papeleta es correcta, con el fin de evitar manipulaciones en las comprobaciones y la pérdida de anonimato mediante la reconstrucción de la papeleta.

A pesar de lo riguroso de la solución propuesta, se han demostrado posteriormente algunas vulnerabilidades como ataques por compra de votos [170] o mediante el uso de los recibos de verificación [171] lo que lo convierte más en una propuesta académica que práctica. A pesar de todo, el sistema podría mejorarse con objeto de evitar este tipo de ataques pero complicando el proceso [169].

Uno de los principales ataques fue diseñado y demostrado por los propios estudiantes del Dr. Rivest. Éste es posible si el número de candidatos por papeleta es elevado, con lo que el número de formas de rellenar las papeletas crece exponencialmente lo que hace posible recuperar la papeleta completa con un número de votantes pequeño y el recibo de uno de ellos [66]. Posteriormente el Dr. Rivest propuso una modificación a su sistema de forma que el número de filas (candidatos) se mantuviera pequeño con respecto al número de votantes.

Otro de los riesgos detectados es la demostración de que es posible obtener un resultado aproximado del recuento final si disponemos de un número determinado de recibos, todo ello antes de que finalice el proceso de votación [172].

Un aspecto muy importante en este sistema es la usabilidad. Si bien es cierto que es posible utilizarlo sin tener que hacer un acto de fe en algún sistema criptográfico más o menos confuso y complejo, ni tener que seguir un curso de aprendizaje de cómo emitir el voto, no es menos cierto que vamos a tener que votar cambiando el chip, de forma que habrá que instruir previamente al votante para dejar claro que votar a favor de alguien es marcar dos veces su nombre y para no votar por alguien hay que marcarlo una vez y todo ello con la necesidad de votar siguiendo las filas.

Con este sistema no solamente obtenemos la comprobación de que el voto es emitido de acuerdo con nuestra voluntad, como los sistemas clásicos o basados en VVPAT, sino que además podemos verificar que ha sido tenido en cuenta aunque no podamos demostrar que el recuento final haya sido correcto. ThreeBallot logra que los votantes puedan verificar su voto y mantener el anonimato, no teniendo que utilizar sofisticados procedimientos basándose en terceros de confianza, ni protocolos que impidan la trazabilidad del voto. El esquema puede que no sea muy práctico tal como se desarrolló inicialmente, pero es de gran importancia teórica, ya que demuestra que es posible diseñar una solución verificable y privada sin apenas uso de la criptografía. Esta solución sigue siendo atractiva por la sencillez de su mecanismo.

4.2.3.6 Conclusiones

Esta propuesta proporciona un alto grado de verificabilidad para los votantes, pudiendo comprobar que sus votos han sido procesados de forma correcta y con un elevado grado de anonimato. También proporciona mecanismos para evitar la manipulación de los votos, ya que puede ser fácilmente detectada.

Esta es la primera vez que la verificabilidad de extremo a extremo (E2E) se ha conseguido sin tener que utilizar complejas técnicas criptográficas. Los principios empleados por ThreeBallot son simples y fáciles de entender. Sin embargo, la resistencia de este diseño a la compra de votos es no tan robusta como el autor esperaba [168]. Por

último destacar que el propio autor ha mejorado su propuesta inicial con ingeniosas modificaciones, denominadas VAV y Twin, que permiten reducir las vulnerabilidades y aumentar la usabilidad del sistema [60].

4.2.4 Scratch&Vote

4.2.4.1 Origen

Esta propuesta del 2006 surgió de la tesis doctoral de Ben Adida dirigida por Ronald Rivest [38]. Al mismo tiempo se publicó un artículo científico firmado por ambos [82]. Por desgracia este desarrollo es una pura propuesta académica que no ha sido puesta a prueba. Además la información disponible es escasa, sobre todo si se compara con el resto de los sistemas.

4.2.4.2 Características

Si hacemos caso a los autores, Adida y Rivest [149], y tienen sobrado prestigio para ello, el sistema Scratch&Vote es el mejor modo de permitir a los votantes comprobar que sus votos han sido procesados correctamente sin necesidad de apoyo por parte de las autoridades electorales. Además esta solución, según descripción de sus desarrolladores, ha sido diseñada para minimizar el coste y aumentar la usabilidad incidiendo en tres aspectos: los votos son en papel y se pueden imprimir utilizando tecnología convencional, son verificables universalmente y además el recuento sólo requiere de un descifrado sencillo, basado en la confianza de las partes. En suma la verificación del proceso por parte del votante puede realizarse incluso antes de emitir su voto.

Esta solución combina propuestas de trabajos anteriores como la posibilidad de seleccionar múltiples candidatos de Baudron [84], la sencillez de la papeleta de Chaum [158] y las técnicas avanzadas de Ryan [61]. La gran diferencia está en el uso de contadores con cifrado homomórfico para el recuento de los votos, en vez de las *mixnets*, por lo que la implicación de la autoridad electoral se limita al descifrado de un sencillo texto cifrado por cada vuelta.

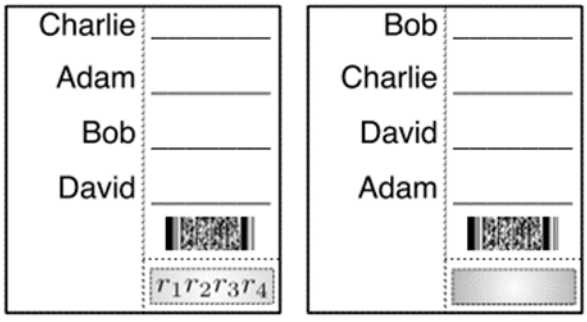


Ilustración 19. Detalle de la papeleta de Scratch&Vote [149].

Scratch&Vote hace que el proceso de verificación por parte del votante sea seguro porque permite que un voto de papel sea revisado sin tener que involucrar a nadie más. Este método introduce la novedad de una superficie de rascado en la parte inferior de la zona en la que aparecen los nombres de los candidatos. El orden en el que aparecen

impresos estos nombres se oculta debajo de esta superficie de rascado y cifrado. Para comprobar que un voto no está alterado, el votante simplemente tiene que rascar la superficie correspondiente para ver el número oculto que guarda una correspondencia con el orden de los nombres de los candidatos. En teoría, los autores dicen que los votantes podrían usar el software criptográfico en la sede electoral o por Internet para verificar este orden, pero explican que es más práctico que entidades de confianza ajenas al proceso proporcionen los medios necesarios para verificarlo. Si el código que posee el elector coincide con el publicado en el *bulletin board*, entonces el voto revisado es legítimo y por tanto habría sido correctamente contabilizado.

La diferencia fundamental está en el uso del cifrado homomórfico que garantiza la imposibilidad de conocer la identidad del votante, pero sí el recuento preciso.

4.2.4.3 Procedimiento de votación

En realidad el votante recibe dos papeletas que a simple vista sólo se diferencian en el orden en el que se muestran los candidatos y decide qué papeleta es la que va a verificar y cuál la que va a utilizar para votar. En la primera "rasca" la superficie dispuesta para ello permitiendo que aparezcan unos dígitos que indican el orden de cada candidato, con los cuales y por medio de una aplicación de descifrado y utilizando una clave pública podrá comprobar que el orden de los candidatos coincide con el impreso en la papeleta y con el descrito en el código de barras, que está cifrado con una clave privada que sólo conoce mancomunadamente la mesa electoral. Esto lo puede realizar incluso antes de votar. Después marcará su elección en la otra papeleta y recortará la zona de la izquierda en la que figuran los nombres de los candidatos, con lo que se garantiza el anonimato. Después se acercará a la mesa de votación y el presidente de la misma comprobará que la superficie de rascado está intacta para evitar la venta de votos y separará esta parte de la papeleta para destruirla inmediatamente evitando que alguien pueda comprometer el secreto del voto. A continuación y mediante escáner óptico se leerá la posición de la marca y el código de barras que cuando se cierre la urna serán publicados con el fin de que el votante pueda comprobar que su voto ha sido tenido en cuenta. Esta información queda protegida dentro de la urna para evitar perder el secreto del voto. Por último el votante se lleva a modo de recibo esta misma parte de la papeleta que utilizará para verificar su voto posteriormente.

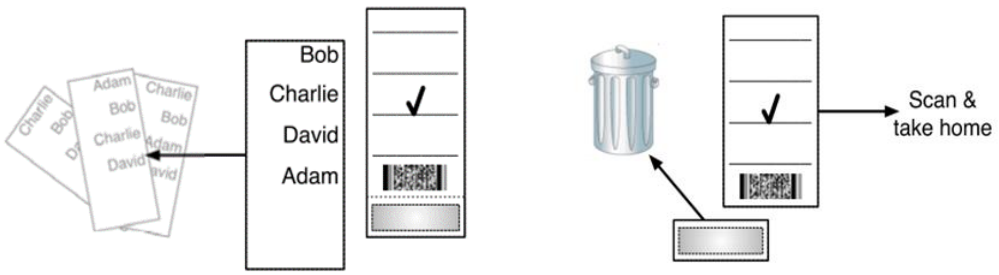


Ilustración 20. Primer y segundo paso de la votación con Scratch&Vote [149].

Para realizar el escrutinio la urna reconoce la posición de las marcas y mediante el código de barras y el algoritmo de descifrado basado en clave privada presente en el equipo y bajo autorización de los integrantes de la mesa, realiza la contabilidad de los

votos. También se pone en el "tablón de anuncios" ya sea en el local o a través de Internet, toda la relación de votos emitidos en la urna, con lo que el votante podrá verificar que el suyo ha sido contabilizado.

El uso del homomorfismo en los procesos electorales fue propuesto por Baudron [84] con objeto de garantizar el anonimato en el recuento de los votos de estructura múltiple debido a que un observador externo no puede sacar conclusiones observando las operaciones homomóficas que se realizan sobre los votos que en ningún caso son descifrados.

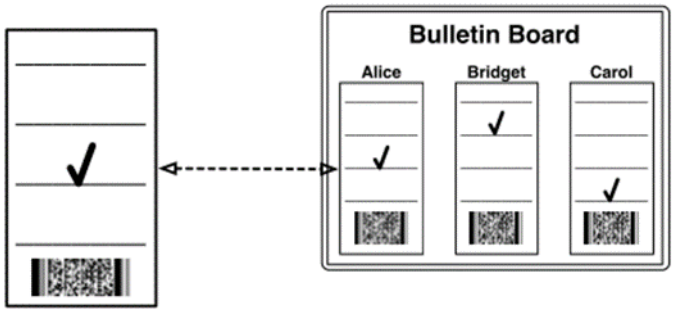


Ilustración 21. Verificación del voto emitido con Scratch&Vote [149].

4.2.4.4 Soporte criptográfico

El uso de la criptografía en esta propuesta es intenso, denso y complejo de describir. Es muy probable que debido a ello no existan a día de hoy estudios comparativos ni descripción de posibles ataques, salvo los que los propios autores describen.

Inicialmente se utiliza el cifrado con clave pública de Paillier [83] que proporciona un cifrado semántico seguro con la característica de disponer de homomorfismo en las operaciones de adición. Para ello se utilizan contadores homomórficos descritos por Baudron [84] que funcionan de tal forma que un observador externo no puede decir qué contador interno ha sido incrementado al recibir el voto pero sí que ha sido tenido en cuenta. En otras palabras, la suma homomórfica utilizada por este sistema puede ser verificada por cualquiera sin desvelar el secreto de anonimato.

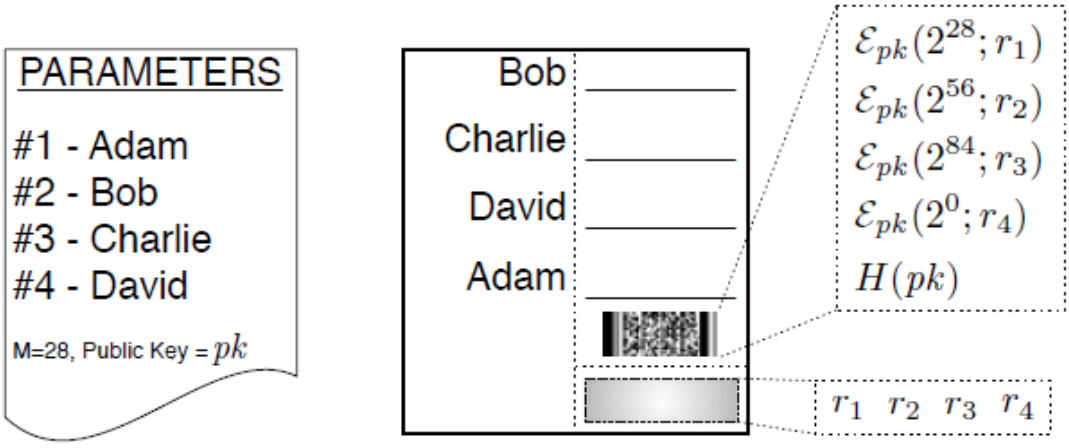


Ilustración 22. Detalle de la información pública y de la papeleta Scratch&Vote [149].

El aspecto fundamental de este sistema está en que los parámetros básicos de las elecciones se publican previamente, indicando el orden de los candidatos, es decir asignando un número a cada uno de ellos, además de la clave pública y M que es la longitud en bits necesaria para representar los valores de los contadores de cada candidato. En la propia papeleta, además del nombre de los candidatos y el espacio a la derecha correspondiente para realizar la marca de selección, está ubicado el código de barras que contiene la información cifrada con la clave pública de la posición de los nombres (r_1,r_2,r_3,r_4) y finalmente y en la parte inferior, una zona que se recorta antes de depositar el voto con la posición de los candidatos en la papeleta, que puede ser utilizada para la verificación de la misma antes de la votación, siendo en este caso la papeleta inválida para votar ya que podríamos conocer a quién ha votado el elector.

Una vez cerrado el proceso de votación, es suficiente para realizar el recuento del voto la interacción entre la información pública del proceso, la posición de la marca y la información cifrada en el código de barras, para supuestamente conseguir un recuento seguro y transparente sin relación ninguna con el votante.

4.2.4.5 Análisis crítico

Uno de los problemas que se presentan en este tipo de votaciones son las vulnerabilidades que las propias papeletas presentan en el proceso de impresión, como ya hemos comentado en casos anteriores. También es cierto que en este caso el votante es el que elige antes y al azar qué papeleta que va a utilizar para votar y cuál para verificar, con lo que no podemos estar seguros de qué papeletas van a ser utilizadas para votar. Además, sólo a posteriori y sobre las papeletas depositadas (leídas previamente por el escáner óptico), se puede demostrar su validez utilizando el mecanismo ya descrito. Este es otro aspecto clave ya que si el escáner óptico tiene memoria secuencial podríamos averiguar qué papeleta ha utilizado cada elector y si los funcionarios electorales acceden a la información que permite crearlas y codificarlas, podría darse una fuga de información sobre el orden de los candidatos en función de las papeletas lo que permitiría relacionar la posición de los candidatos en cada papeleta con el votante que la ha depositado y por tanto romper el secreto del voto. Los propios autores no lo descartan si se conocieran de antemano los detalles de la impresión de las papeletas, pero no sería sencillo. Evidentemente se puede reducir la vulnerabilidad si se controla el proceso de impresión y se protege mediante algún tipo de ocultamiento del código de barras de la misma con el fin de que no esté visible.

Más fácil sería alterar la superficie de rascado de los votos o leer su contenido y reponer la superficie. No se ha experimentado en este terreno en la práctica para poder establecer si es factible o no.

Si un funcionario electoral y algunos de los votantes se confabulan para quedarse con la parte de rascado del voto, en lugar de desecharla y eliminarla, el votante podría ser capaz de revelar el sentido de su voto al funcionario y más tarde a una tercera parte.

Otro ataque más sofisticado y complejo de evitar es el denominado "coacción aleatoria". Se basa en forzar a los votantes a señalar en todo caso una posición determinada de la papeleta sin importar a quién se beneficia. De esta forma se garantiza que los votos bajo coacción se reparten aleatoriamente, beneficiando a los partidos mayoritarios en esa zona. A los sistemas similares como el PunchScan y el Prêt à Voter les ocurre lo mismo.

Gran parte del buen funcionameinto del sistema está en la seguridad del tablón de anuncios en el que se publican los votos procesados en cada urna. Por supuesto la primera

necesidad es garantizar que el acceso esté disponible y no se vea afectado por un ataque de denegación de servicio. Por otro lado los datos publicados deben estar certificados por algún mecanismo como firmas digitales que garanticen que son los correctos.

4.2.4.6 Conclusiones

Esta solución está basada en un complejo soporte criptográfico, cuyos detalles sólo están al alcance de verdaderos expertos. Además no existen pruebas reales por lo que desconocemos sus resultados prácticos. Su manejo por parte del votante no parece complejo y puede ser implementada con tecnología actual a bajo coste. Lo que es más importante, cualquier votante puede verificar su propio voto y su uso es intuitivo ya que estamos acostumbrados a las superficies de rascar y descubrir.

En cualquier caso la usabilidad, como se desprende de la descripción del proceso de votación, no es buena y la accesibilidad para personas con algún tipo de diversidad funcional, ya sea visual o motora es muy baja por la cantidad de manipulaciones necesarias sobre la papeleta.

4.2.5 Prêt à Voter

4.2.5.1. Origen

Este esquema fue propuesto por Peter Ryan de la Universidad de Luxemburgo entre el 2004 y el 2006 y lo denominó Prêt à Voter [173] [61] [174], pero la idea inicial fue propuesta en colaboración con David Chaum [175]. Posteriormente se desarrolló una implementación para un concurso-votación en el 2007 [176] en el que quedó en segundo lugar después de PunchScan pero ganó en el apartado de mejor diseño. Actualmente el proyecto sigue vivo bajo la denominación *Trustworthy Voting Systems* [177] con el trabajo de dos grupos de investigadores de las Universidades de Surrey y Birmingham y el apoyo de la de Luxemburgo. Pretenden construir un prototipo completo y confiable, demostrando su fiabilidad en los cálculos y operaciones matemáticas de aleatorización y cifrado seguro. Su fecha de conclusión está fijada para este año (2014).

4.2.5.2. Características

En esencia es un sistema de votación que utiliza escaneo óptico del voto y un modelo criptográfico basado en *mixnets*. Se fundamenta en que en una mitad del voto aparecen los nombres de los candidatos en un orden aleatorio que es destruida antes de votar y en la otra mitad aparecen las casillas de selección para que el votante señale el candidato que desee. Esta última mitad contiene un número de serie que permite bajo circunstancias controladas averiguar a qué candidato se ha votado y le sirve al votante como recibo de verificación.

En su desarrollo práctico se ha utilizado para una votación de estudiantes en un entorno de concurso denominado VoComp que se realizó en julio de 2007 en Oregon [159]; el equipo responsable de su puesta en marcha reconoció haber aprendido varias lecciones de los errores cometidos en su diseño. Uno de los más importantes fue utilizar una función para generar los códigos aleatorios sin los requisitos de seguridad necesarios, como quedó reflejado en las conclusiones de este concurso. También fue probado en la Universidad de Newcastle en mayo del 2007 con la intención de mejorar su usabilidad y fiabilidad [178], donde quedaron patentes las múltiples debilidades y dificultades de uso

de este tipo de procedimientos de votación, tanto en la lectura óptica en sí, como en el mecanismo de consulta en el tablón de anuncios. A pesar de todo la valoración final fue positiva.

4.2.5.3. Procedimiento de votación

El votante, antes de proceder a emitir el voto, retira la columna de la izquierda de la papeleta con el nombre de los candidatos y la destruye en presencia de los miembros de la mesa para preservar el secreto del voto. A continuación el votante se dirige a la urna que en realidad dispone de un escáner óptico, el cual lee el voto con la marca de selección y el número de serie único que figura en la parte inferior de la papeleta, que servirá posteriormente para recuperar mediante una clave secreta el orden de los candidatos en esa papeleta y también para poder verificar que el voto ha sido correctamente contabilizado mediante un tablón de anuncios (*bulletin board)* en el que se publican todos los votos emitidos con su número de serie. Después de que el voto sea leído se procede a firmar digitalmente el archivo escaneado, por parte de la mesa electoral, y el votante se queda con esta mitad del voto que no contiene los nombres de los candidatos de las casillas de selección.

Candidates	Mark X
Idefix	
Asterix	X
Panoramix	
Obelix	
	3994025096

Ilustración 23. Configuración básica de la papeleta Prêt á Voter [61].

La principal complicación de este sistema es cómo asegurar que la información cifrada en el número de serie de la papeleta permite recuperar con seguridad y sólo en el momento del recuento el orden original de los nombres de los candidatos, sin establecer nexo alguno con el votante.

Mark X
.
X
.
.
3994025096

Ilustración 24. Recibo básico del Prêt á Voter [61].

Existen dos mecanismos para verificar los votos. Por una parte cada votante puede comprobar que su voto ha sido tenido en cuenta comparando su recibo con el listado de los votos emitidos que se publican en el tablón de anuncios, mediante el cual verifica que ha sido procesado. Por otra parte los auditores del sistema pueden verificar que todos los votos emitidos han sido publicados y correctamente descifrados, gracias al mecanismo criptográfico que recupera la posición de los candidatos.

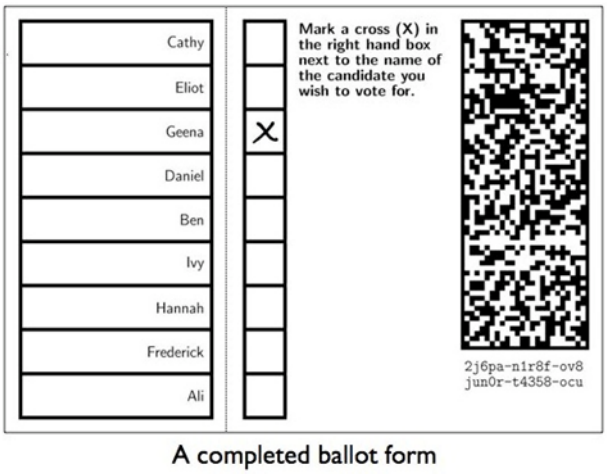


Ilustración 25. Papeleta real de votación del Prêt à Voter [173].

Desde el punto de vista del votante el proceso de votación tiene varios pasos:

- Emitir el voto. Para ello debe recoger una papeleta, marcar su elección en la columna de la derecha, cortar la parte izquierda y destruirla de alguna forma fehaciente para que no sirva de instrumento que demuestre lo que se ha votado y escanear la parte derecha en la urna electrónica.
- Comprobar, con ayuda de la mesa y de forma opcional una papeleta con el fin de comprobar que el número de serie de la misma permite recuperar el orden de los candidatos.
- Verificar el voto, reteniendo la parte derecha del mismo (o una copia) una vez escaneado a modo de recibo con el objeto de comprobar que coincide con el que aparece en el tablón de anuncios una vez cerrada la votación. Así mismo puede ser utilizado como prueba en caso de impugnación de la votación si no apareciera o se mostrara modificado.

4.2.5.4. Soporte criptográfico

La idea básica de este sistema es que los votos emitidos están cifrados de la misma forma que aquellos que son descifrados previamente para comprobar su correcto funcionamiento y la imposibilidad de realizar la trazabilidad sobre los mismos, incluidas las autoridades electorales. Para ello se utilizan tres pasos que pueden realizarse separados o combinados y son: el mezclado o barajado de los votos, el descifrado y el recuento. Para verificar el proceso se eligen al azar y públicamente una serie de votos, que son utilizados para demostrar que el proceso es fiable y preciso. El proceso de comprobación previo para confirmar el correcto funcionamiento del sistema, en ningún caso pone al descubierto

los detalles del procedimiento pero permite al votante comprobar que su voto ha sido grabado como él ha elegido y posteriormente ha sido contabilizado como fue depositado, aspecto este que en principio sólo está garantizado por el correcto diseño del algoritmo de cifrado/descifrado.

Para ello utiliza una forma particular de permutación por desplazamiento cíclico de la lista de candidatos que se repite en varias ocasiones formando varios procesos continuados de cifrado en forma de "capas de cebolla" impidiendo el proceso inverso salvo que se conozca el algoritmo completo, al cual nadie tiene acceso directamente, salvo el sistema en el momento del recuento cuando es activado mancomunadamente por los miembros de la mesa.

Al igual que en el caso del PunchScan la codificación entre las capas se hace cifrando las referencias con RSA, constituyendo las denominadas *tellers* que son unas tablas cifradas encargadas de enlazar la información entre las diversas capas, es decir son *mixnets*. Estas *tellers* permiten la progresión del cifrado en un sentido pero la impiden en sentido contrario salvo que se conozcan las claves. De esta forma se impide relacionar las marcas leídas por el OCR con la posición de los candidatos u opciones de la papeleta en concreto. El número de serie de la papeleta es el encargado de iniciar el cifrado de la posición de los candidatos, de tal forma que aun conociendo este número y la posición de las marcas es inviable recuperar la lista original, aun en el caso de conocer los detalles del encriptado. Para poder recorrer las capas en sentido contrario con el objeto de realizar el recuento es necesario conocer las diversas claves entre cada capa.

4.2.5.5. Análisis crítico

Existen varias posibilidades de ataque. Si se dispone antes de la votación de algunos votos, estos podrían ser utilizados para coaccionar a los votantes formando una cadena de votación controlada, entregando al votante un voto ya marcado adecuadamente y recibiendo del votante otro nuevo para continuar con la cadena. También se podría forzar a los votantes a marcar siempre la misma posición en las papeletas (ataque por aleatorización).

En cualquier caso y como en otros sistemas, la complicación está en la impresión previa de las papeletas en número y forma predefinida. También es un punto débil el hecho de que la mesa electoral disponga de mucha información sobre el proceso. Otra debilidad es el hecho de que el votante conserve la parte izquierda del voto y pueda demostrar a quién ha votado. Para ello el proceso debería obligar al votante a destruir esa parte del voto delante de la mesa o facilitar el acceso a falsas partes izquierdas para evitar la coacción al votante.

Como en el resto de los sistemas que utilizan OCR el diseño de las papeletas está supeditado a conseguir una lectura segura, lo que obliga a dejar en segundo plano los aspectos de usabilidad con respecto al votante. Además se ha venido demostrando que el reconocimiento de caracteres automatizado no es 100% preciso, ya que las marcas escritas a mano no lo son.

A pesar de todo es uno de los mejores diseños y tiene muchas posibilidades de convertirse en una solución con futuro.

4.2.5.6. Conclusiones

Puede parecer que el diseño de Prêt à Voter es excelente y que la papeleta es intuitiva y fácil de usar, es decir dispone de una usabilidad destacable. Esa fue la conclusión del concurso VoComp comentado anteriormente, pero en la prueba

desarrollada en el 2007 quedó claro que el votante no entiende con claridad los pasos necesarios para votar con este sistema y la necesidad de alguno de ellos, lo que da como resultado una baja calificación en su usabilidad [178]. No obstante debemos considerar relativa esta conclusión ya que en la mayor parte de los otros sistemas no se ha realizado este tipo de estudios.

Evitar que el votante elija la papeleta que va a ser utilizada para votar no parece producir mayor problema, como tampoco entregar a cada votante una copia digitalizada de su papeleta, en lugar del original, obligando a una comparación en tiempo real. Como en todos los sistemas similares, pueden aparecer problemas en la lectura por parte de los OCR.

Una fortaleza de esta solución es la posibilidad de retar al sistema eligiendo una papeleta para ello y otra para votar. Esto además puede poner al descubierto errores o debilidades en el sistema de cifrado de los votos. También es cierto que los votantes no necesitan unos conocimientos ni instrucciones previas complejas para la votación.

La generación de números aleatorios es una debilidad del método descubierta por el equipo Punchscan en la competición VoComp. Supone un error de diseño grave que habrá que resolver de una forma innovadora y definitiva, lo que resultaría muy beneficioso para el sistema.

Otros ataques posibles son:

- Robar papeletas antes de las elecciones y utilizarlas para coaccionar a los votantes.
- Realizar un ataque de aleatorización, forzando a los ciudadanos a votar de una forma aleatoria, exigiéndoles que marquen siempre una misma posición en la papeleta, con lo que se beneficia al partido mayoritario.

Otro problema en este tipo de soluciones es la cadena de custodia sobre las papeletas, antes y durante la votación. También es un punto débil la impresión de las mismas en cuanto que tiene que estar perfectamente controlado para evitar que se conozcan los detalles de la generación del orden de los candidatos y su relación con los números de serie. No descartamos la posibilidad de que alguien manipule la impresión para generar errores en la emisión de las papeletas.

Es importante separar las papeletas utilizadas para comprobar el correcto funcionamiento del proceso, de las que se van a utilizar para votar. En particular supondría un problema contra el secreto del voto utilizar una copia de una papeleta que haya sido usada para votar y posteriormente proceder con la copia a su verificación, descubriendo de esta forma el sentido del voto. Esto se puede evitar comprobando en el momento del escaneo que el número de serie no haya sido utilizado previamente.

El sistema permite en su última versión una papeleta de opción múltiple e incluso con orden de preferencia, haciendo figurar un número en vez de una simple marca [176].

4.2.6. Bingo Voting

4.2.6.1. Origen

Lo primero sería justificar la presencia de este sistema en esta tesis ya que está fuera de las corrientes predominantes en este ámbito, claramente influidas por los expertos norteamericanos que han sido referenciados hasta este momento. Lo cierto es que nos puede servir para equilibrar la balanza con la presencia de otro desarrollo europeo junto con el anteriormente descrito (Prêt á Voter), que lo es en parte, ya que el resto de los

presentados son norteamericanos. Además tenemos el apoyo documental de una excelente tesis doctoral del 2012 de Christian Henrich [179].

El Bingo Voting es un sistema de votación electrónica que fue introducido en 2007 por Jens- Matthias Bohli , Jörn Müller- Quade y Stefan Röhrich pertenecientes al Instituto de Seguridad y Cifrado (IKS) adscrito al Instituto de Tecnología de Karlsruhe (KIT) en Alemania. [151]. En 2008 fue galardonado con el premio alemán sobre seguridad de la Fundación Horst Görtz. Posteriormente se introdujeron mejoras basadas en la tesis doctoral de Christian Henrich. En ésta se presenta la versión original del Bingo, se describe la experiencia adquirida durante la primera elección en el mundo real llevado a cabo en las elecciones de los representantes de los estudiantes de la Universidad de Karlsruhe en el 2008 y propone varias mejoras para abordar algunas deficiencias y debilidades. Se intenta demostrar que es una alternativa posible y práctica a las elecciones tradicionales con papel.

4.2.6.2. Características

La primera novedad es que la votación se desarrolla sobre una urna electrónica tipo DRE que después de la elección del votante emite un recibo. Por tanto no hay papeletas de papel. La urna utiliza un generador de números aleatorios para cifrar los votos y para su emisión se usan dispositivos de confianza, así denominados por los autores, como podrían ser una pantalla táctil y una impresora laser. Igualmente esencial son sus recibos en papel sin información sobre el sentido del voto, lo que viene a denominarse "recibo anti-coacción" (freeness receipt), para evitar la compra de votos y la intimidación pero que permiten al votante verificar que su voto fue procesado correctamente. En este recibo sólo figuran los nombres de los candidatos con un número a continuación. Por tanto todo el proceso de votación, se desarrolla sobre una urna electrónica con una interfaz gráfica genérica y una impresora de recibos.

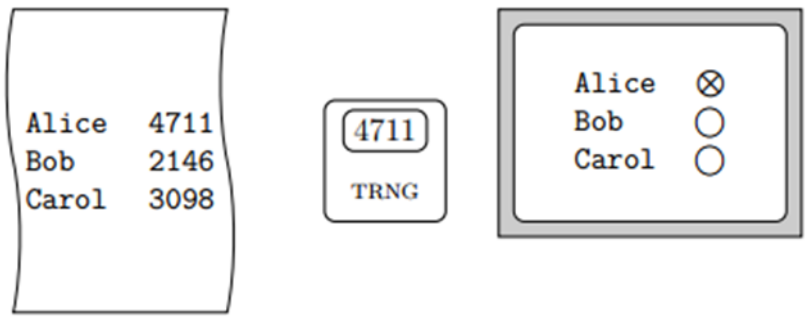


Ilustración 26. Detalle del proceso del Bingo Voting. A la izquierda el recibo, en el centro el número aleatorio reciente generado por la urna y a la derecha la opción escogida por el votante [179]

La idea central de Bingo Voting es que la urna cifre la elección del votante mediante la generación de números aleatorios para cada una de las opciones (ver figura). Hay dos tipos de números aleatorios en el proceso, los números aleatorios "ficticios" (dummy) generados antes de la fase de votación y números aleatorios "recientes" (fresh) que se generan durante el proceso de votación mediante el generador de números aleatorios de

confianza. El número aleatorio utilizado para codificar la elección final del votante se genera como número aleatorio "reciente" y es mostrado por el generador de números aleatorios de confianza dentro de la cabina de votación. El resto de los números en el recibo del votante son números aleatorios "ficticios".

Los números aleatorios ficticios son los números que aparecen en el recibo y que además no se corresponden con ninguna elección del votante. Es importante recalcar que estos números se fijan antes de que comience la fase de votación. Si suponemos una elección en la que participen N votantes (donde cada votante puede emitir un único voto), cada candidato tendrá inicialmente N números aleatorios ficticios distintos.

Los números aleatorios recientes (generados durante la fase de votación por el generador de números aleatorios de confianza) son los que se utilizan para identificar en el recibo la elección realizada por el votante en la urna electrónica en el momento de la votación. El algoritmo utilizado para la generación de estos números recientes, que son los que finalmente aparecerán en el recibo del votante señalando la opción escogida, no garantiza que anteriormente no hayan sido utilizados en el grupo de los ficticios, es decir, que no hayan sido generados antes. Si esto ocurriera se denominan "colisiones" (una en el caso de 100.000.000 votantes, con una longitud de los números aleatorios de 30 bits y con una probabilidad de ser detectada del 0,99995).

4.2.6.3. Procedimiento de votación

En la descripción del proceso de votación es fácil imaginar que todo depende del engaño que establecemos al considerar que los votos ficticios puedan representar votos reales. En la fase de preparación de la votación se adjudican el mismo número de votos ficticios a cada candidato. Durante la fase de votación y cada vez que un votante elige al candidato Z, ese candidato NO pierde un voto ficticio ya que es reemplazado por un número aleatorio reciente. Esto significa que el candidato Z tiene ahora un voto ficticio MÁS que los otros candidatos. Por esta razón, el número de votos ficticios que le quedan a cada candidato se traduce directamente en el resultado del recuento, si al comienzo de la votación cada candidato tenía tantos votos ficticios como votantes.

Para que todo funcione como se espera tenemos que garantizar dos cosas. Lo primero es que podamos demostrar que todos los candidatos dispongan inicialmente del mismo número de votos ficticios y la autoridad electoral lo pueda comprobar. Este valor debería ser como mínimo igual al número máximo de votantes, pero podría ser superior sin problema. El segundo aspecto que es necesario cuidar es que cada vez que se vota por un candidato hay que restar un voto ficticio, ni más ni menos.

En cambio para demostrar que por cada voto emitido no se le descuenta uno ficticio al candidato elegido, deben darse dos pasos. Primero, para generar el recibo, la urna imprime un número aleatorio ficticio al lado de cada candidato no votado y un número aleatorio reciente al lado del nombre del candidato votado y que es calculado por el generador de números aleatorios recientes en ese instante. El votante es capaz de comprobar esto, comparando la pantalla del generador de números recientes con lo impreso en el recibo, de forma que ese número debe aparecer al lado del nombre de su candidato. En un segundo paso, el votante puede verificar por medio de la publicación que hace la autoridad electoral al final del proceso y mediante el listado de todos los números ficticios que no han sido "consumidos" y por tanto utilizados para el recuento, que cada número que figura al lado de cada candidato en su recibo no está incluido en la lista y por tanto cada uno de ellos ha "consumido" un voto ficticio o bien ha utilizado un número "reciente". Esto da lugar a una comprobación que puede resultar laboriosa e

incluso inviable si los listados son muy largos debido al números de votantes y de candidatos.

Antes de la fase de votación la autoridad electoral publica los requisitos de la votación. Esto incluye la lista de candidatos y el número de votos ficticios asociados a cada uno de ellos. Se supone que la máquina que genera los números ficticios utiliza el mismo sistema que para los números aleatorios recientes, aunque estos últimos utilizan un algoritmo que intenta impedir la repetición de los ya generados.

Suponiendo una elección en la que participen N votantes y donde cada votante puede emitir un voto, dicha máquina generará N números aleatorios ficticios en función del número de votantes para cada candidato y guardará este conjunto de números ya que es necesario para realizar el recuento y generar los recibos. Es importante recalcar que además del conjunto de votos aleatorios ficticios, la máquina de votación lleva a cabo una prueba para mostrar que cada candidato ha recibido el mismo número de votos ficticios. Además el número de votos ficticios debe coincidir exactamente en todos los candidatos y debemos garantizar que en ningún caso este listado pueda hacerse público. Sólo entonces puede comenzar la fase de votación.

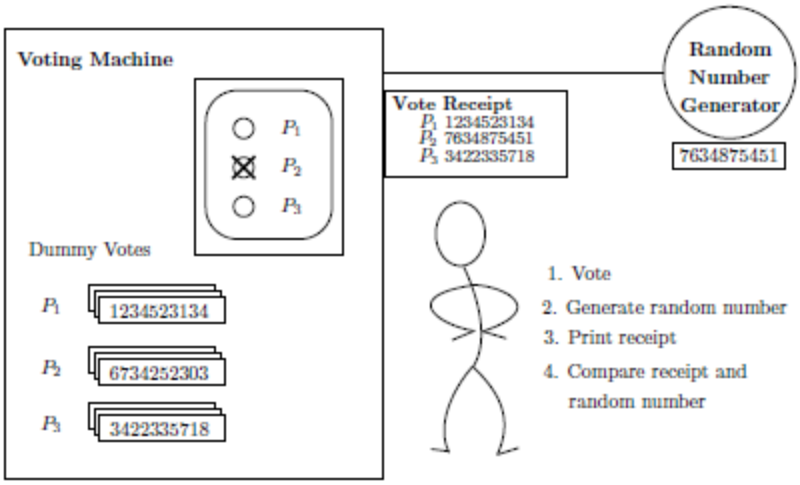


Ilustración 27. Detalle del proceso de votación con Bingo Voting [151].

El votante una vez verificada su identidad entrará en la cabina de votación y activará el sistema mediante una *smart card* (el lector está en la parte derecha de la ilustración 28) y se encontrará con una mesa con una pequeña impresora para emitir el recibo, la máquina de votación tipo DRE con pantalla y ratón y el generador de números aleatorios recientes conectado a la máquina de votación (segundo por la izquierda en la ilustración). Después emite su voto con ayuda del ratón (en este caso Alice) e inmediatamente después el generador de números aleatorios recientes proporciona un número para el candidato elegido (4711 en la ilustración 26). El elector lo verifica y presiona la opción de VOTAR y se imprime un recibo asignando el número aleatorio reciente al candidato elegido. En este punto es importante señalar que Alice no pierde un voto ficticio por lo que tiene un voto ficticio más comparado con el resto de candidatos que sí los "consumen" y de esta forma podemos realizar posteriormente el recuento.

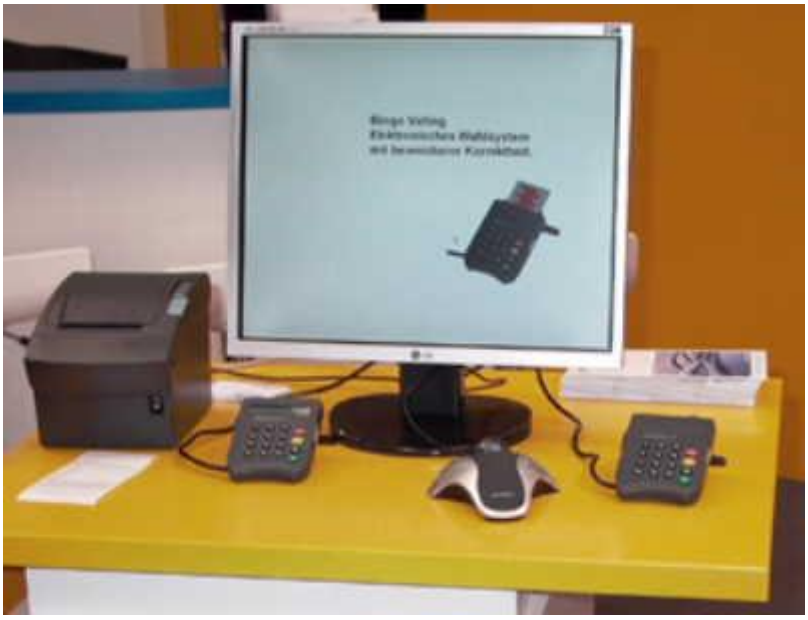


Ilustración 28. Aspecto de la urna de votación del Bingo Voting. (Univ. Karlsruhe **[180]**).

¿Cómo verifica el usuario que su voto ha sido emitido correctamente? Comparando el número visualizado en la pantalla del generador de números aleatorios de confianza con el número asociado al candidato que él ha elegido. Sólo el votante sabrá quién ha sido el candidato elegido ya que para cualquier otra persona ese número es indistinguible de los números aleatorios ficticios.

Durante la fase de recuento la autoridad electoral publica tres conjuntos de datos distintos:

• Una copia digital de cada recibo emitido durante la fase de votación. De esta forma cada votante puede verificar que su voto fue emitido y publicado correctamente.

• Se demuestra para cada recibo publicado que contiene la cantidad correcta de números aleatorios de cada tipo, es decir, que todos menos uno (el número aleatorio reciente) son números aleatorios ficticios. Esta comprobación la hace la mesa electoral mediante un proceso cerrado y supuestamente fiable.

• La autoridad electoral publica todos los números aleatorios ficticios que no fueron utilizados durante el proceso de votación. Estos votos se denominan votos ficticios restantes y son los que se utilizan para hacer el recuento.

Lo verdaderamente importante es que el número de los votos ficticios restantes para cada candidato tiene correspondencia inversa con el número de votos que este candidato recibió durante la fase de votación, a partir del cual obtenemos directamente el recuento de ese candidato.

¿Cómo se obtiene el recuento? En primer lugar, restando al número de votos ficticios de cada candidato, el número de personas que no votaron, es decir, el número de votantes para los que la autoridad electoral creó números aleatorios ficticios pero que no fueron utilizados. Estos datos pueden ser calculados a partir del número de recibos publicados que equivale obviamente al número de votos emitidos. En segundo lugar, el número de números aleatorios ficticios que le quedan a cada candidato será el número de votos recibidos por cada uno de ellos.

¿Cómo tener en cuenta los votos en blanco y votos inválidos?

◦ Lógicamente si no se ha elegido candidato en el voto, en el recibo no debería existir ningún número aleatorio reciente, por lo que el comprobante sólo tendrá números

ficticios asociados a los candidatos que habrían sido utilizados por todos ellos. Inmediatamente marcaríamos la papeleta como un voto en blanco que habría que tener en cuenta como un voto que no se contabiliza para ningún candidato. Otra opción sería crear un "candidato en blanco".

◦ Como no es posible que el recibo contenga más de un número aleatorio reciente, esta opción no existe.

Existen dos tipos de verificaciones, la individual y la global.

La verificación individual tiene dos partes:

- En la primera de ellas, durante la fase de votación, el votante comprueba que en su recibo se codifica correctamente el candidato seleccionado, comparando el número aleatorio generado en ese momento por el generador de confianza y que es asignado al candidato elegido en el recibo que recoge el votante.
- En la segunda, después de la fase de votación, el votante verifica que su recibo se ha publicado correctamente. Si el recibo emitido durante el proceso de votación es idéntico al recibo publicado posteriormente por la autoridad electoral, puede deducirse que el voto fue incluido en el recuento, aunque no tenemos garantías de que haya sido contabilizado correctamente.

Para cumplir con la verificación global la autoridad electoral tiene que comprobar:

- Que cada candidato cuenta al principio de la votación con idéntico número de votos ficticios y esto se lleva a cabo mediante una comprobación aleatoria parcial.
- Que cada recibo está correctamente creado y que todos los números son ficticios salvo uno, o dicho de otra forma, que cada candidato no votado perdió como máximo un número ficticio por cada votante. Esto se realiza verificando que todos los números aleatorios del recibo menos uno son ficticios mediante un procedimiento que los miembros de la mesa pueden ejecutar.
- Que cada número ficticio generado inicialmente figura en un recibo (ha sido consumido) o bien está publicado como no utilizado en el proceso (ficticios restantes).
- Por último ha de comprobarse que el número de coincidencias (colisiones al generar los números aleatorios) es mínimo y que en ningún caso puede afectar al resultado.

4.2.6.4. Soporte criptográfico

El núcleo de esta votación se fundamenta en el carácter imprevisible del generador de números aleatorios de confianza (TRNG) y en los estrictos compromisos de privacidad entre el voto y el votante. Para ello es esencial que todos los números aleatorios ficticios sean únicos y esta es la razón de la comprobación de todos los números ficticios generados en la fase de preparación. De esta forma es bastante sencillo detectar las posibles repeticiones al generarse aleatoriamente los números recientes. Si no podemos asegurar la unicidad, es importante al menos asegurar que habrá muy pocas repeticiones, ya que cada colisión significa un voto potencialmente modificado. Esto debe ser comprobado en cada mesa mediante un procedimiento que se ejecutará antes de la votación. El número de colisiones que se considera aceptable se determina por el número de votos que pueden cambiarse sin alterar el resultado de la elección, pero pueden existir.

Como la mayoría de los sistemas de votación con verificación de extremo a extremo, este exige la publicación de los datos que permitan verificar la exactitud de los resultados y convencer a los votantes de que su voto se incluyó correctamente en el recuento. Para ello se publican los números ficticios restantes mediante un servicio web y una copia de cada uno de los recibos.

El recibo anti-coacción se basa en la imposibilidad de distinguir entre números aleatorios ficticios consumidos y los recientes, así como en el cuidado aislamiento de la cabina de votación y de la urna que se utiliza para votar.

Es evidente que en este sistema es crítico el diseño del generador de números aleatorios y por ello originalmente se propuso un sistema mecánico como los utilizados en el juego del bingo. Ahora la propuesta es generarlos a partir de una tarjeta criptográfica. Para que el método funcione correctamente, los números aleatorios ficticios deben ser calculados de forma que puedan verificarse antes de que comience la fase de votación. En cuanto al recibo anti-coacción, debe mantenerse en secreto qué número aleatorio es el reciente y cuáles se han generado antes de la votación. Para garantizar estas propiedades el sistema utiliza un esquema de compromisos mediante un algoritmo denominado UHDLC.

También es importante para el correcto funcionamiento que todos los números aleatorios sean únicos y ésta puede ser una debilidad ya que el sistema no lo garantiza. Dado que cada repetición puede significar que un voto ha sido modificado, el número de repeticiones queda fijado por el número de votos que pueden cambiarse sin alterar el resultado de la votación. Esta información se publica al final del recuento.

4.2.6.5. Análisis crítico

Una posible ventaja es que el procedimiento es relativamente sencillo en su uso. Tras haber seleccionado el votante a su candidato y emitir y confirmar el voto, el ordenador se comunica con el generador de números aleatorios de confianza y recibe un número aleatorio reciente para el candidato seleccionado en cada voto emitido. Acto seguido se imprime un recibo y el votante tiene que comparar los números aleatorios obtenidos en la pantalla con los números impresos en el recibo.

Una de las principales limitaciones del sistema sería un elevado número de candidatos o de votantes. Por otro lado existe una vulnerabilidad conocida como ataque *Babble* (balbuceo) que consiste en que el elector, que está bajo coacción, pasa vía radio o mediante fotografía la información completa, es decir, todos los números ficticios del voto antes de generarse el número reciente para verificar posteriormente que el número ficticio que no se imprime en el recibo coincide con uno de los publicados al final del proceso.

También pueden producirse otros errores:

1) El recibo no coincide con lo seleccionado por el votante. Es obvio que esto sólo lo puede indicar el votante en el momento en que se genera el recibo y nunca podremos estar seguros de que no fue un problema provocado por el votante. Una posible solución es cambiar el interfaz de la urna electrónica de una pantalla a un escáner óptico que mantiene la papeleta fuera del alcance del votante hasta que éste dé su visto bueno al voto, momento en el que el recibo es entregado al elector y contabilizado. En cualquier caso para poderlo demostrar se rompe la privacidad del voto. Otra solución sería aplicar la propuesta del sistema Scantegrity e imprimir a un lado de la papeleta un código de barras que permitiría relacionar el recibo entregado con el voto realmente

emitido. Sin duda esto complicaría el proceso de votación y la usabilidad del sistema.

2) El recibo del votante no coincide con los publicados. En este supuesto lo primero que tenemos que demostrar es que el recibo exhibido por el votante es el original y no ha sido manipulado. Para ello podríamos incluir en el recibo una firma digital añadiendo una tarjeta con firma digital en la impresora del recibo. Claro que de esta forma no podría verificarse la autenticidad del recibo hasta el momento de la verificación posterior al recuento.

La posibilidad de que existan colisiones en la generación de los números aleatorios debería estar acotada en valores que no afecten al resultado.

El hecho de que las autoridades electorales puedan conocer detalles sobre el procedimiento de generación de los números aleatorios es una debilidad del método.

4.2.6.6. Conclusiones

Posible pérdida de la privacidad. El esquema propuesto permite a los votantes y autoridades electorales detectar y avisar de las manipulaciones sobre los votos, en cambio no ofrece ningún mecanismo de recuperación sin violar la privacidad del voto. Esto significa que una sola manipulación detectada puede obligar a los responsables electorales a anular la elección completa lo que implica una gran pérdida de tiempo y dinero.

Elecciones complejas. Este sistema de votación tiene problemas cuando el número de candidatos elegibles es grande, ya que el tamaño de los recibos crecerá provocando serios problemas de usabilidad. Al mismo tiempo se incrementarán las posibilidades de que aparezcan repeticiones (colisiones). Paralelamente la longitud de los números aleatorios crecerá y sin duda plantearía problemas en la fase de comprobación. No debemos olvidar que la cantidad de números aleatorios que contiene un recibo tiene que ver con el número de opciones que un votante tiene y con el número de votantes que hay en la elección. El coste de la implementación e impresión en los recibos puede aumentar de forma muy importante. Por otra parte, se alargará considerablemente el tiempo de votación ya que por cada voto que se emita, el elector debe localizar un número específico en el recibo y compararlo con el de la pantalla del generador de números aleatorios recientes. Probablemente sería muy interesante realizar un estudio para determinar el número máximo de candidatos y de votantes permitidos con el objetivo de que el sistema pueda funcionar correctamente sin pérdida exagerada de tiempo, ni incremento del coste en su implementación, ni de usabilidad.

Confianza en generación de los números aleatorios. La suposición más importante para el Bingo Voting es que el generador de números aleatorios genere realmente números al azar y sin repeticiones. En la práctica, la aleatoriedad está basada en un generador de números aleatorios digital que no llega a ser del todo convincente. Probablemente utilizar algún método robusto, fiable y rápido para generar aleatoriedad aumentaría la credibilidad del sistema.

Votación múltiple. Este esquema puede presentar problemas cuando el votante tiene que emitir más de un voto en las elecciones. En las pruebas que hasta el momento se han desarrollado no se han tenido en cuenta los problemas reales que pueden generar estos casos.

Colisiones. La longitud de los números aleatorios usados en una elección de este tipo tiene que ser elegida de modo que las colisiones sean muy poco probables. Evidentemente esto se consigue aumentando considerablemente la longitud de los números aleatorios, pero esto presenta una clara desventaja, ya que de nuevo (como

ocurría en las elecciones complejas) aumenta el tiempo que el votante pasa dentro de la cabina de votación comparando su voto con el recibo.

4.3. Comparaciones entre las soluciones

4.3.1. Punchscan.

Este sistema ha sido comparado con el Prêt à Voter y con ThreeBallot por Kelsey et al., desde un punto de vista de ataque a los sistemas basados en papel [181] y con Prêt à Voter en un intento de uso en elecciones por correo [182]. En el primer caso se ha demostrado cómo las autoridades electorales pueden cambiar votos sin ser detectados y en el segundo se han puesto de manifiesto los riesgos de utilizar este método en casa para enviar el voto por correo convencional o incluso escaneando el voto en el propio domicilio y enviándolo por Internet. También se podría desarrollar un sistema para poner en entredicho la verificación del proceso si se tiene oportunidad de acceder a votos en blanco para cambiar una de las hojas del voto emitido (la que no se destruye). En este caso las autoridades no podrían verificar si es la hoja correspondiente o no, ya que pondrían en riesgo el secreto del voto. Esto puede evitarse, como ya se ha comentado, si es un proceso aleatorio el que determina qué hoja ha de ser destruida.

4.3.2. Scantegrity.

El Scantegrity sólo ha sido comparado con su antecesor, el Punchscan [165]. Aunque el primero es más sencillo, la esencia de ambos tiene mucho que ver con los procesos químicos de la tinta empleada y no están exentos de coacción si el votante es requerido para entregar el número de serie de la papeleta y el código de votación y a su vez se tiene acceso al listado completo de códigos ocultos de todas las papeletas, que en principio sólo están disponibles para los administradores electorales.

4.3.3. ThreeBallot.

Esta solución ha sido comparada y estudiada a pesar de ser una propuesta eminentemente académica, quizá por lo novedoso del sistema sin apenas criptografía o bien por la destacada figura de su autor [183]. El propio autor lo compara con otras dos variantes de la propuesta que no han sido estudiadas: VAV y Twin. El primero utiliza las tres partes de la papeleta con un esquema fijo: voto a favor (V), voto en contra (A), voto a favor (V); cada voto en contra anula un voto a favor. La solución Twin es más compleja ya que el votante se lleva el recibo de comprobación que pertenece a otra papeleta. Lo más destacable es que es un sistema que permite la verificación del proceso electoral sin depender de soporte criptográfico ni de complejos equipamientos [60].

El estudio comparativo más claro y preciso es el desarrollado por miembros del Departamento de Informática de la Universidad de Bergen [183], en el que se evidencian las debilidades y vulnerabilidades a posibles ataques.

4.3.4. Scratch&Vote.

El Scratch&Vote ha sido comparado con el Punchscan y el Prêt á Voter debido a la similitud en las papeletas utilizadas. Con respecto al primero existe una similitud en cuanto a las diversas capas utilizadas en el voto y en el segundo caso con la papeleta dividida en partes separables.

En estos dos casos existen aspectos verificables, uno que la papeleta ha sido almacenada tal y como ha sido depositada y dos, que ha sido correctamente procesada. En ambos casos el votante aleatoriamente elige una parte de la papeleta para depositarla en la urna, bien la parte superior o inferior en el Punchscan o bien separando los nombres de las marcas mediante la separación física de ambas. De esta forma no se revela la elección del votante, manteniendo el anonimato del voto. Posteriormente y una vez emitidos todos los votos, se pueden contabilizar los mismos y permitir que el votante lo verifique mediante la reconstrucción parcial del voto original, gracias a información en poder de la autoridad electoral y sin dar cabida a la posibilidad de demostrar cuál es exactamente su papeleta evitando la coacción sobre el votante. En estos dos casos es el votante el que elige qué parte del voto o qué voto elige para ser emitido, lo cual garantiza antes de la votación y al 50%, que las papeletas no han sido amañadas.

4.3.5. Prêt à Voter.

Esta solución es similar a las que utilizan *mixnets*, como el PunchScan y el Scantegrity y han sido comparadas entre sí en el VoComp resultando ganadora la primera debido al hallazgo de un error en la programación de un *flag* en el generador de números aleatorios del Prêt à Voter que fue corregido posteriormente.

También ha sido comparada con ThreeBallot [183] con la conclusión de que ambas tienen debilidades comunes, como la posibilidad de reconstruir la papeleta original mediante diversos tipos ataques ya descritos, pero que pueden ser evitadas con contramedidas sencillas.

4.3.6. Bingo Voting.

Ha sido comparado con el PunchScan [151] quedando claro que éste es menos robusto en lo que se refiere a la protección contra la coacción, ya que el Bingo Voting tiene un diseño que evita ese tipo de ataques como hemos descrito anteriormente.

En comparación con Prêt à Voter, este tiene una gran ventaja ya que sólo obliga al votante a utilizar los aspectos criptográficos del esquema de votación después de haber hecho su elección. Para Bingo Voting los pasos adicionales después de la emisión del voto son necesarios para garantizar la exactitud de los votos que es lo que intentamos verificar.

5

5. Conclusiones y aportaciones generales con relación a los objetivos. Trabajos futuros.

"Basta con que el pueblo sepa que hubo una elección,
los que emiten los votos no deciden nada;
los que cuentan los votos lo deciden todo."

Iósif Stalin

5.1. Conclusiones generales

Las dudas iniciales eran: ¿hasta qué punto merece la pena complicar el proceso electoral introduciendo la tecnología con sus riesgos y limitaciones? ¿Por qué si los procesos electorales son estables y adecuados si se gestionan de una forma clásica, damos por sentado que van a mejorar por el mero hecho de introducir la tecnología? ¿Son los sistemas basados en E2E la solución definitiva para el VE?

Después de todo este estudio y disertación, creo que el uso de las TIC en el voto electrónico puede estar justificado en aquellos casos y circunstancias en los que aporte más beneficios que riesgos, aunque estos estén presentes, como por ejemplo en procesos de consultas o votaciones en entidades, asociaciones, organismos, empresas o cualesquiera otras de menor entidad. También puede ser conveniente en caso de que sea necesario garantizar el recuento electoral en un tiempo prudencial como ocurre en países cuyas características orográficas o demográficas impidan o dificulten el cumplimiento de este requisito. Esta necesidad podría afectar al estricto cumplimiento de los considerados aspectos básicos del proceso electoral democrático, si bien en ningún momento deberíamos de tolerar que la fiabilidad global del proceso sea puesta en duda.

Podemos deducir que alcanzar la solución perfecta en el uso de la tecnología en los procesos electorales sigue la evolución de una curva asintótica en la que, a pesar del tiempo y de los esfuerzos de la comunidad científica, el acercamiento a las garantías necesarias es demasiado lento y no se vislumbra como posible. Sí es cierto que los aspectos de fiabilidad y posibilidad de verificación individual y general han mejorado de

forma importante pero en detrimento de la usabilidad y con un incremento notable de la dificultad de la puesta en marcha y gestión del proceso de votación. Otra recomendación sería intentar desarrollar las soluciones con módulos lo más genéricos posible para fomentar la reutilización del código y la flexibilidad en el uso de la solución; por ejemplo a la hora de utilizarla en procesos electorales diversos, con una vuelta, con dos, con prelación de las selecciones, etc. También sería buena idea utilizar técnicas de seguimiento de errores y refinamiento de la programación aspecto este que, a tenor de los resultados y versiones, no ha sido tenido en cuenta. Sin embargo el sistema de votación debería hacer todo lo que dice que hace y nada más que lo que dice que hace.

A lo largo de esta tesis, creo que ha quedado claro que la brecha entre la teoría y la práctica es muy importante y el único método efectivo para reducirla es implementar las soluciones, evaluarlas y mejorarlas con pruebas reales. Esto lleva tiempo y mucho esfuerzo de investigación y desarrollo y en la mayor parte de las soluciones presentadas no parece que haya sido así. La implementación de la teoría aunque sea elaborada rigurosamente descubre sorpresas inesperadas. Las escasas experiencias de validación de las soluciones y comparación entre ellas, salvo la experiencia del VoComp, no permiten el desarrollo de conclusiones más prácticas y útiles.

Sería necesario antes de cada proceso electoral comprobar bajo circunstancias reales que el sistema va a funcionar y que la propia esencia del sistema se puede ver alterada de un instante a otro por un mal funcionamiento de cualquiera de los elementos. Por ello sería muy importante habilitar procedimientos de contingencia en función de la gravedad del problema. Para abaratar costes y facilitar el mantenimiento y sustitución de los elementos es muy recomendable el uso de equipamiento lo más genérico posible. Los sistemas tienen que ser capaces de adaptarse a una gran variedad de procesos electorales con rapidez y bajo coste. Por lo que es esencial un diseño flexible. Siempre hay que tener perfectamente delimitados y contemplados todos los posibles errores en una votación y gestionarlos con transparencia, publicarlos y explicarlos al elector y al público en general.

En cuanto a las soluciones con verificación E2E que he analizado intentan proteger el registro del voto tal y como fue emitido pero son menos rigurosas con el proceso de recuento. Parece quedar claro que los aspectos más reforzados con el E2E son: la posibilidad de verificar el proceso electoral y preservar el voto emitido de cualquier tipo de manipulación, aunque no sea tan cuidadoso con la posibilidad de añadir votos. El pilar fundamental de los sistemas E2E es la verificabilidad tanto individual como universal. La primera abre la posibilidad de que cada votante compruebe que su voto se registra según su deseo impidiendo la demostración de ello a un tercero, siendo su responsabilidad y de nadie más. La segunda capacita a cualquier observador genérico, ya sea votante, interventor o autoridad electoral, para poder verificar que el recuento de todos los votos registrados es correcto gracias a la publicación de todos los votos emitidos. Combinando ambos tipos de verificación conseguimos un proceso electoral con verificación abierta. Además este aspecto proporciona una mayor integridad al sistema. La debilidad más evidente de estas soluciones es que siempre hay alguien que tiene en sus manos una parte del secreto del proceso, en general una clave compartida, que podría ser utilizada para conculcar alguno de los principios básicos de un proceso democrático mediante colusión entre varios responsables del proceso electoral (miembros de la mesa, autoridades, responsables técnicos, etc.). El éxito de estos sistemas dependerá no solo de sus características de seguridad sino de la complejidad de los mismos, aunque toda esta complejidad no sea suficiente para asegurar que el voto sea secreto. Si bien el secreto del voto es una condición ineludible, no es menos importante la fiabilidad del recuento. El principal determinante para la adopción de este tipo de métodos de votación, y en general de cualquier otro, es que los oficiales de las elecciones lo entiendan y lo acepten y que

los votantes se den cuenta de sus beneficios. Aunque curiosamente los legisladores ya han puesto su confianza en software que no entienden, son reticentes a utilizar estos nuevos métodos. Se da la paradoja de que, para hacer unas elecciones más transparentes, es necesario el uso de criptografía que hace más complejos y oscuros los procesos subyacentes.

Otro de los problemas cruciales de la verificación E2E es que si algo falla, ya sea el procedimiento de verificación de los códigos, el descifrado para el necesario recuento o la publicación de los recibos en el tablón de anuncios, falla todo el proceso y no queda otro remedio que volver a votar, aunque quizá pueda permitirse una cierta tolerancia ante los fallos como en cualquier otro sistema (sea o no de votación), incluidos los de votación tradicional.

La posibilidad de riesgos y vulnerabilidades presentes en cualquier proceso electoral no desaparece completamente con los métodos E2E, incluso pueden aparecer otros nuevos, aunque obtenemos la ventaja de un recuento rápido y de poder verificar que éste ha sido correcto. Sin duda ganamos en rapidez sin perder la opción de la verificación.

La capacidad de entender con claridad los fundamentos criptográficos del voto electrónico E2E es muy reducida y solo está al alcance de unos pocos, que son los que proponen y critican los diversos métodos. Esto hace que las propuestas solo provengan de un limitado grupo de especialistas, sin duda capaces, pero limita enormemente el avance rápido y eficaz de este tipo de soluciones. Además complica de forma importante la formación, no ya del ciudadano que los tiene que utilizar, sino también de las autoridades electorales que los tienen que poner en marcha y administrar.

Los métodos E2E presentan soluciones a los problemas de verificación en el voto electrónico, pero incrementan otros problemas como la usabilidad, la accesibilidad, la formación previa de las autoridades electorales y de los votantes, la complejidad de la puesta en marcha y la complicada impresión de las papeletas. En cualquier caso, queda demostrado que un grupo de personas que se pongan de acuerdo entre ellas y tengan algunas responsabilidades en el proceso electoral pueden manipular los resultados a pesar de todas las complicaciones criptográficas que se utilicen y en este sentido no se han propuesto soluciones a día de hoy, aunque me consta que se está trabajando en ello. Evidentemente esto también puede acontecer en los procesos electorales convencionales, pero conviene dejar claro que por mucha tecnología y criptografía que se utilice no es garantía suficiente de seguridad ante la manipulación de resultados o la posibilidad de ejercer coacción sobre el votante. De hecho recientemente los investigadores Moran y Naor demostraron cómo atacar al votante coaccionándolo, si se le permitía escoger la hoja-recibo que permanecía en su poder en función de determinadas características de la papeleta entregada [184]. También en este caso queda claro que, si alteramos la impresión de los recibos que se llevan los votantes, les podemos hacer creer que han votado por una opción diferente a la realmente emitida. Y, cómo no, se nos dan las pistas para poder comprar votos o coaccionar al votante utilizando la cámara de los teléfonos móviles o similares.

Como hemos visto, en la mayor parte de los casos de votación E2E la seguridad e integridad del sistema depende de forma muy importante del procedimiento de votación, que debe estar diseñado para evitar que la picaresca y el ingenio en la manipulación del proceso externo de votación puedan poner en riesgo todo el entramado criptográfico que hay detrás. Algunas de estas vulnerabilidades pueden evitarse si la custodia de las papeletas es estricta y el acceso del votante a las mismas está correctamente diseñado y controlado.

En resumen, los sistemas basados en E2E tienen a su favor la verificabilidad, la integridad, la precisión y la privacidad, aunque en este último aspecto me pregunto hasta

que punto es secreto el voto cuando el recibo que conserva el votante mantiene referencias con el voto emitido mediante números o códigos ópticos, de tal forma que puede ponerse en tela de juicio si el votante está votando de forma estrictamente secreta. Si a esto añadimos el hecho de que las autoridades electorales tienen la clave que une el recibo con el voto emitido, podemos concluir que el secreto está condicionado y no es absoluto. Por otra parte y en cuando a sus debilidades, podemos hablar de una puesta en marcha y gestión compleja, un coste alto, una accesibilidad muy pobre y una usabilidad que condiciona de forma importante su manejo sencillo y correcto. Pero además, la enorme y compleja carga criptográfica que hay detrás aleja al ciudadano de una votación clara e intuitiva como a las que está acostumbrado.

A pesar de todo y hoy por hoy, las propuestas de VE basadas en E2E son las que mejor cumplen con los requisitos exigidos. Después de todo lo expuesto podemos deducir que el grado de cumplimiento de los criterios básicos de un proceso de votación en función de los diversos tipos de urnas podría ser el señalado en la tabla 1.

	Urna clásica	Correo postal	DRE	VVPAT con acceso a la papeleta	VVPAT sin acceso a la papeleta	E2E
Inviolabilidad	*****	***	***	****	*****	***** (1)
Privacidad	*****	*	***	**	*****	****
Anti-coacción	*****	*	****	*	*****	***** (1)
Integridad	*****	***	***	****	****	*****
Verificabilidad	*****	*	**	*****	****	*****
Usabilidad	****	***	**** (1)	***	** (1)	*** (1)
Versatilidad	****	****	****	****	***	*** (1)
Accesibilidad	***	**	***** (1)	***	** (1)	**
Coste	****	***	**	**	**	**
Rapidez en el recuento	*** (1)	*** (1)	*****	*** (2)	*** (2)	*****

Tabla 1. Relación entre cumplimento de criterios y tipos de urnas

(1) Con un buen diseño y en el mejor de los casos.
(2) En el caso de tener que verificar la urna.

5.2. Aportaciones: tabla y comparativa final

Los criterios de valoración son los determinados como necesarios en el apartado 2.4. de esta tesis, a los que se han añadido los de versatilidad (capacidad de adaptarse con facilidad y rapidez a diversos entornos de votación), accesibilidad (capacidad de adaptarse a las diversidades funcionales del votante) y coste (gasto necesario para desplegar y utilizar la solución). Las valoraciones se hacen con una calificación en número de estrellas en función del grado de cumplimiento estimado, de tal forma que una estrella (*) indica un cumplimiento muy pobre, dos estrellas (**) señala un cumplimiento pobre, tres estrellas (***) se equipara a un cumplimiento básico del criterio, cuatro estrellas (****) como correcto, cinco estrellas (*****) como destacado y seis (******) como excelente.

En el caso del PunchScan y del Scantegrity, existe cierto grado de dependencia de los miembros de la mesa para verificar el proceso electoral, que aunque no se fundamenta en información que ellos conozcan, ya que el usuario puede comprobar directamente que

se ha procesado su voto correctamente, esto sólo se puede asegurar después del cierre de la votación y por ello si existiera una impugnación podría poner en jaque todo el proceso electoral en esa mesa. Pero además tenemos el problema de los rotuladores especiales necesarios para proceder con la elección.

En Scratch&Vote la comprobación se puede realizar utilizando la información pública del proceso electoral, sin necesidad de las autoridades electorales e incluso previamente, seleccionando una papeleta al azar para realizar una verificación previa. Para ello se rascaría la superficie diseñada al efecto, descubriendo los datos de la asignación aleatoria entre los nombres y las posiciones en la papeleta. Posteriormente, este orden en la disposición de los nombres en la papeleta se cifra utilizando la información pública del proceso electoral. Por último este texto cifrado resultante se compara con el código de barras presente en la papeleta con el fin de demostrar su coincidencia. En este aspecto, esta solución permite la verificación sin ayuda y de forma previa a la votación, pero complica enormemente la impresión de las papeletas y la gestión del proceso.

Considero la propuesta Prêt à Voter como la mejor solución de las estudiadas, aunque tiene problemas de seguridad con el PRNG y además sea necesaria la participación de las autoridades electorales para poder verificar el proceso, ya que lo ideal sería que los votantes pudieran estar seguros de que su voto se contabilizó como lo emitieron sin tener que confiar en ellas. A continuación está PunchScan que además ha sido valorada como la mejor en los concursos como el VoComp, aunque no fue comparada nunca con la primera. Después aparecen Bingo Voting y Scratch&Vote, destacando ligeramente la primera por versátil y original. En los últimos puestos han quedado Scantegrity, muy penalizada por depender de un proceso químico con las tintas que le resta transparencia y usabilidad y ThreeBallot que a pesar de su sencillez y originalidad soporta una colección de vulnerabilidades aunque apenas ha sido utilizada.

	PunchScan	Scantegrity	ThreeBallots	Scratch&Vote	Prêt á Voter	Bingo Voting
Inviolabilidad	****	****	***	****	****	****
Privacidad	****	****	*****	*****	****	*****
Anti-coacción	****	*****	****	****	*****	****
Integridad	*****	*****	****	*****	*****	****
Verificabilidad	*****	*****	****	*****	*****	****
Usabilidad	**	**	**	*	***	**
Versatilidad	**	**	**	**	***	***
Accesibilidad	**	*	**	*	**	***
Coste	**	*	***	**	***	**

Tabla 2. Comparativa de los sistemas de votación basados en E2E

Si observamos la tabla 2, podemos deducir que ninguna de estas soluciones alcanza la excelencia en cuanto a inviolabilidad ya que el secreto no lo es al estar siempre al alcance de unos pocos e incluso en la mayor parte de ellos figura un número de serie único en la papeleta, lo que podría conculcar el requisito de anonimato. Lo mismo ocurre, en mayor o menor grado, con la usabilidad, versatilidad, accesibilidad y coste. Obviamente el aspecto que sale mejor valorado es la verificabilidad y no podría ser de otra forma. Además, los aspectos de integridad, diseño anti-coacción y privacidad se mueven entre lo suficiente y lo destacable, dependiendo de la propuesta.

En la práctica son las soluciones Scratch&Vote y Prêt à Voter las únicas viables ya que PunchScan y Bingo Voting han desaparecido y, desde mi punto de vista, es Prêt à Voter la que mayores oportunidades tiene de ser implementada de forma práctica en un futuro cercano.
Por último incluimos la tabla 3 con el resumen de los aspectos técnicos más importantes de las soluciones estudiadas.

	PunchScan	**Scantegrity**	**ThreeBallots**	**Scratch&Vote**	**Prêt á Voter**	**Bingo Voting**
Equipo para emisión del voto	OCR	OCR	OCR	OCR	OCR	DRE específico
Cifrado utilizado	PRNG + MIXNETS + SHA 256	PRNG + MIXNETS	Bajo nivel	Homomórfico	Mixnets (tellers)	TRNG + UHDLC
Tipo de papeleta utilizado	Doble normal	Doble con tintas especiales	Normal triple	Doble con parte de rascado	Doble con código óptico	Sin papeleta
Tipo de recibo para el votante	Mitad de la papeleta	Mitad de la papeleta	Un tercio de la papeleta	Menos de la mitad de la papeleta	Mitad de la papeleta	Generado por impresora
Información publicada en el bolletin board	Parcial	Parcial	Completa	Completa con código de barras	Parcial	Parcial (números ficticios restantes)
Características especiales	Rotulador de marcado especial	Rotulador con tinta especial		Posibilidad de verificación pre-votación	Posibilidad de verificación pre-votación	Posibilidad de colisiones

Tabla 3. Resumen de los aspectos técnicos de las soluciones E2E

5.3. Trabajos futuros

Hay tres razones por las que merece la pena seguir con el análisis, la valoración y la comparación en la evolución de estos sistemas:

- La continua mejora en las propuestas que denota el alto nivel de los autores y su capacidad de auto-crítica, que sin duda nos presentarán soluciones cada vez más sencillas, usables y robustas.
- La aparición de nuevas propuestas, en las que ya se está trabajando, que evitarán la necesidad de la presencia de autoridades electorales para el proceso de recuento, impidiendo así que nadie pueda aunque sea parcialmente conocer las claves del método de descifrado. De esta forma evitaríamos que la colusión entre estos responsables pusiera en peligro los requisitos necesarios en un proceso electoral con garantías democráticas.
- La posibilidad de desarrollo de alguna variante de estas soluciones que pudiera ser utilizada para voto remoto.

Queda mucho trabajo por hacer en esta materia y sigue siendo tan apasionante como el primer día. Sin duda en algún momento seremos capaces de encontrar una solución que satisfaga a todos, cumpla con los requisitos necesarios y genere CONFIANZA en el electorado. El único camino posible, hoy por hoy, es la utilización de soluciones basadas en procesos de verificación abiertos y universales.

REFERENCIAS

[1] L. Panizo, A. Alonso y A. Yuste, «Votobit proceedings 2003-2004 eVoting reports,» Asociación de Investigación Instituto Automática y Fabricación, León, España, 2004.

[2] L. Panizo, Aspectos tecnológicos del voto electrónico, Lima, Perú: Oficina Nacional de Procesos Electorales, Gerencia de Capacitación, Investigación y Asistencia Técnica Electoral, Subgerencia de Capacitación e Investigación Electoral, Área de Investigación Electoral, 2007.

[3] M. Torre y L. Panizo, «Technological Solutions for Electronic Voting and Guarantees of the Integrity of the Electoral Process. A Case Study,» 10 10 2012. [En línea]. Available: http://hdl.handle.net/10612/2845. [Último acceso: 09 12 2013].

[4] L. Panizo, «Aspectos tecnológicos del voto electrónico,» de *Democracia digital, participación y voto electrónico*, Valencia, España, Fundación CEPS, 2010, p. 200.

[5] H. Alaiz, L. Panizo, R. A. Fernández y J. Alfonso, «Technical Audit of an Electronic Polling Station: A Case Study,» *International Journal of E-Services and Mobile Applications (IJESMA),* vol. 3, nº 3, p. 15, 2011.

[6] AETICAL, «Plataforma voto-e,» Proconsi, 2012. [En línea]. Available: http://votoe.es. [Último acceso: 13 07 2013].

[7] Florida Department of State, «Official Results November 7, 2000,» 07 11 2000. [En línea]. Available: http://election.dos.state.fl.us/elections/resultsarchive/SummaryRpt.asp?ElectionDate=11/7/2000&Race=PRE&DATAMODE. [Último acceso: 13 08 17].

[8] A. Shapiro, Compositor, *Absentee Ballots Go Missing in Florida's Broward County.* [Grabación de sonido]. http://www.npr.org/templates/story/story.php?storyld=4131522. 2004.

[9] A. Gumbel, Steal This Vote: Dirty Elections and the Rotten History of Democracy in America, Nations Books, 2005.

[10] A. D. Rubin, «http: //avirubin.com/,» October 2004. [En línea]. Available: http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=132x2913485. [Último acceso: 20 5 2013].

[11] R. Mercuri, «Voting-machine risks,» *Commun. ACM,* vol. 11, nº 35, p. 138, 1992.

[12] S. Chasteen, «Electronic voting unreliable without receipt, expert says,» *Stanford Report,* pp. http://news.stanford.edu/news/2004/february18/aaas-dillsr-218.html, 18 02 2004.

[13] R. F. Celeste, D. Thornburgh y H. Lin, «Asking the right questions about electronic voting,» *National Academies Press,* 2006.

[14] R. C. Hite, «Electronic voting offers, opportunities and presents challenges.,» U.S. Govermment Accountability Office, Washington, 2004.

[15] C. McCormack, «Re-counting the vote: What does it cost? Pew Charitable Trusts,» 01 10 2010. [En línea]. Available: http://www.pewstates.org/uploadedFiles/PCS_Assets/2010/Pew_Cost_of_Recounts_report.pdf. [Último acceso: 13 07 2013].

[16] Saveour Votes, «Analysis of the Cost of Procuring and Implementingan Optical Scan Voting System in Maryland.,» 04 03 2011. [En línea]. Available: http://www.saveourvotes.org/reports/2010/2010-3-04sov-costanalysis.pdf. [Último acceso: 13 07 2013].

[17] I. D. Fernández, «El voto electrónico.,» *Revista del Ilustre Colegio de Abogados de Madrid,* 2003.

[18] M. Cantijoch , «El voto electrónico ¿ un temor justificado ?,» *TEXTOS de la Cibersociedad ,* nº 7, 2005.

[19] C. Cox y A. Rubin, «Is the U.S. ready for electronic voting?,» *New York Times Upfront,* 20 09 2004.

[20] R. Mercuri, «www.notablesoftware.com/,» 2001. [En línea]. Available: www.notablesoftware.com/RMstatement.html. [Último acceso: 27 08 2013].

[21] T. Kohno, A. Stubblefield, A. A. Rubin y D. S. Wallach, «Analysis of an electronic voting system,» *Security and Privacy,* pp. 27 - 40, 2004.

[22] C. Armen y R. Morelli, «E-voting and computer science,» de *ACM ITiCSE´05*, Monte de Caparica, Portugal,, 2005.

[23] A. Di Franco, A. Petro, E. Shear y V. Valdiimirov, «Small vote manipulations can swing elections,» *Communications of the ACM,* vol. 47, nº 10, pp. 43-45, 2004.

[24] J. Carracedo Gallardo, Seguridad en redes telemáticas, Madrid: McGRAW-HILL, 2004.

[25] Council of Europe Committee of Ministers, *Legal, operational and technical standards for e-voting, rec(2004),* Bruselas: Council of Europe Committee of Ministers, 2004.

[26] J. Carracedo Gallardo y E. Pérez Belleboni, «Voto electrónico, voto telématico y voto por Internet: requisitos socialmente demandados y técnicamente viables.,» de *Democracia digital, participación y voto electrónico*, Valencia, Fundación Centro de Estudios Políticos y Sociales, 2010, p. 200.

[27] E. Belleboni, Aplicación de documentos de identificación electrónica a un esquema de voto telemático a escala paneuropea, seguro, auditable y verificable. Tesis doctoral, Madrid: Universidad Politécnica, 2013.

[28] Gobierno de España, Ministerio del Interior. Dirección general de política interior., 2010. [En línea]. Available: http://www.infoelectoral.mir.es/EnlacesInteres/enlaces_mae.html. [Último acceso: 2013 5 26].

[29] H. K. Prasad, J. A. Halderman, R. Gonggrijp y et al., «Security Analysis of India's Electronic Voting Machines,» de *17th ACM Conference on Computer and Communications Security (CCS '10)*, Chicago, 2010.

[30] A. B. Filho y M. A. Cortiz, Fraudes e Defesas no voto electronico, Sao Paulo, Brasil: All Print , 2006.

[31] M. Torre y L. Panizo, «buleria.unileon.es,» 10 10 2012. [En línea]. Available: http://hdl.handle.net/10612/2845. [Último acceso: 2013 09 14].

[32] R. Mercuri, Electronic Vote Tabulation: Checks and Balances., Philadelphia: PhD thesis, University of Pennsylvannia, 2001.

[33] K. Daimi, K. Snyder y R. James, «Requirements Engineering for E-Voting Systems.,» *Software Engineering Research and Practice,* pp. 259-265, 2006.

[34] S. Ikonomopoulos, C. Lambrinoudakis, D. Gritzalis, S. Kokolakis y K. Vassiliou, «Functional requirements for a secure electronic voting system.,» de *Security in the Information Society: Visions and Perspectives, IFIP TC11 17th International Conference on Information Security (SEC2002)*, Cairo,Egypt, 2002. .

[35] G. Z. Qadah y R. Taha, «Electronic voting systems: Requirements, design, and implementation.,» *Computer Standards & Interfaces,* pp. 376-386, 2007.

[36] M. Volkamer y M. Mcgaley, «Requirements and evaluation procedures for evoting,» de *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference* , Viena, Austria, 2007.

[37] K. Weldemariam, A. Mattioli y A. Villafiorita, «Managing Requirements for E-Voting Systems: Issues and Approaches.,» de *Requirements Engineering for e-Voting Systems (RE-VOTE), 2009 First International Workshop* , Atlanta, Georgia, 2009.

[38] B. Adida, Advances in cryptographic voting systems, Massachusetts: Thesis (Ph. D.)--Massachusetts Institute of Technology, Dept. of Electrical Engineering and Computer Science., 2006.

[39] R. L. Rivest , A. Shamir y Y. Tauman, «How to leak a secret,» de *Proceedings of the 7th International conference on the theory and application of cryptology and information security: Advances in cryptology*, Gold Coast, Australia, 2001.

[40] D. Aranha, M. M. Karam, A. Miranda y F. Scarel, «Software Vulnerabilities in the Brazilian Voting Machine,» de *Electronic Voting Tech. Workshop*, Bellevue, Washington, 2012.

[41] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati y S. K. Sakhamuri, « Security analysis of India's electronic voting machines,» 2010. [En línea]. Available: http://indiaevm.org/evm_tr2010.pdf . [Último acceso: 2013 06 06].

[42] R. L. Rivest, «Some thoughts on electronic voting,» 26 5 2004. [En línea]. Available: http://people.csail.mit.edu/rivest/pubs.html#Riv04a. [Último acceso: 25 5 2013].

[43] B. Schneier, «Opendemocracy,» 09 11 2004. [En línea]. Available: http://www.schneier.com/essay-068.html. [Último acceso: 16 07 2013].

[44] D. W. Jones y B. Simons, Broken ballots: Will your vote count in electronic age?, Stanford, California: CSLI Publications, 2012.

[45] B. Schneier, «www.schneier.com,» 10 11 2004. [En línea]. Available: https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html. [Último acceso: 08 09 2013].

[46] El Periódico, «http://www.elperiodico.com/es/noticias/barcelona/20100522/bcn-pagara-indra-hasta-que-justifique-sus-errores/print-272858.shtml,» *BCN no pagará a Indra hasta que justifique sus errores,* 22 05 2010.

[47] La voz de Galicia, «file:///C:/Users/Usuario/Desktop/Una%20auditor%C3%ADa%20externa%20analizar%C3%A1%20los%20fallos%20en%20las%20elecciones%20a%20la%20Polic%C3%ADa.htm,» *Una auditoría externa analizará los fallos en las elecciones a la Policía,* 21 06 2011.

[48] D. W. Jones, «Threats to Voting Systems,» de *Workshop on Developing an Analysis of Threats to voting systems (N.I.S.T.)*, Gaithersburg, Maryland, 2005.

[49] A. Appel, «Security seals on voting machines: A case study,» *ACM Trans. on Information and System Security ,* vol. 14, nº 2, 2011.

[50] J. Kelsey, «Strategies for software attacks on voting machines,» de *NIST workshop on Threats to Voting Systems*, Gaithersburg, MD, 2005.

[51] D. Wagner, J. A. Calandrino, A. J. Feldman, A. J. Halderman y et al., «Source code review of the Diebold Voting System,» Universidad de Berkeley, Berkeley, California, 2007.

[52] H. Hursti, «Diebold TSx evaluation: Security alert. Technical report ,Black Box Voting,» 11 05 2006. [En línea]. Available: http://www.blackboxvoting.org/BBVreportIIunredacted.pdf. [Último acceso: 13 07 2013].

[53] RAE, Diccionario de la Lenguaje Española, Vigésima segunda edición ed., Madrid: Real Academia Española, 2001.

[54] B. Adida y A. Neff, «Ballot Casting Assurance.,» de *2006 USENIX/ACCURATE Electronic Voting Technology (EVT) workshop*, Vancouver, Canada, 2006.

[55] J. Benaloh, Verifiable Secret-Ballot Elections. PhD thesis, New Haven : Faculty of Graduate School, Yale University, 1996.

[56] C. A. Neff, «A verifiable secret shuffle and its application to e-voting,» *Proceeding CCS '01 Proceedings of the 8th ACM conference on Computer and Communications Security,* pp. 116-125, 2001.

[57] R. Cramer, R. Gennaro y B. Schoenmakers, «A Secure and Optimally Efficient Multi- Authority Election Scheme,» *Lecture Notes in Computer Science,* vol. 1233, 1997.

[58] B. Schoenmakers, «Fully auditable electronic secret-ballot elections,» de *Informatik*, Mannheim, Germany, 2000.

[59] D. Chaum y et al., «Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting,» *IEEE Security & Privacy,* vol. 6, nº Mayo-junio, pp. 40-46, 2008.

[60] R. L. Rivest y W. D. Smith, «Three voting protocols: ThreeBallot, VAV,and Twin,» de *EVT'07 Electronic Voting Technology Workshop*, Boston, 2007.

[61] P. Y. Ryan, «Pret a voter with a human-readable, paper audit trail.,» de *Frontiers of Electronic Voting*, Schloss Dagstuhl, Germany, 2007.

[62] B. Schneier, «Voting security and technology,» *Security & Privacy, IEEE,* vol. 2, nº 1, p. 84, 2004.

[63] Scantegrity, «http://scantegrity.org/,» [En línea]. Available: http://scantegrity.org/. [Último acceso: 29 01 2014].

[64] M. Kutyłowski y F. Zagórski, «Verifiable Internet Voting Solving Secure Platform Problem,» de *Advances in Information and Computer Security. Lecture Notes in Computer Science Volume 4752*, Berlin, Springer Berlin Heidelberg, 2007, pp. 199-213.

[65] D. Chaum, «Blind Signature Systems,» de *Advances in Cryptology*, Santa Barbara, CA, Springer US, 1984, p. 153.

[66] D. W. Jones, «http://homepage.cs.uiowa.edu/~jones/voting,» 2009. [En línea]. Available: http://homepage.cs.uiowa.edu/~jones/voting/E2E2009.pdf. [Último acceso: 04 12 2013].

[67] Observatorio del voto electrónico, «http://www.votobit.org/,» votobit.org, [En línea]. Available: http://www.votobit.org/archivos/participaespaniol.pdf. [Último acceso: 03 12 2013].

[68] United States Election Assistance Commission, «Voting system perfomance guidelines,» 2005. [En línea]. Available: http://www.eac.gov/assets/1/workflow_staging/Page/124.PDF. [Último acceso: 21 01 2014].

[69] Verified Voting, «https://www.verifiedvoting.org,» verifiedvoting.org, [En línea]. Available: https://www.verifiedvoting.org/verifier/. [Último acceso: 03 12 2013].

[70] J. H. Saltzer, D. P. Reed y D. D. Clark, «End-to-End Arguments in System Design,» *ACM Trans. on Computer Systems (TOCS),* vol. 2, nº 4, pp. 277-288, 1984.

[71] J. Kempf y R. Austein, «citeseerx,» 2004. [En línea]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.374.1064. [Último acceso: 24 01 2014].

[72] Demotek, «http://www.euskadi.net,» 24 05 2006. [En línea]. Available: http://www.euskadi.net/botoelek/euskadi/informes/sistemademotek.pdf. [Último acceso: 17 08 2013].

[73] D. W. Jones, «End-to-End Standards for Accuracy in Paper-Based Systems,» de *Workshop on Election Standards and Technology*, Washington DC., 2002.

[74] D. W. Jones , «Taxonomy of threats to voting systems,» 2005. [En línea]. Available: http://homepage.cs.uiowa.edu/~jones/voting/nist2005.shtml. [Último acceso: 08 07 2013].

[75] R. Mercuri, « Explanation of voter-verified ballot systems,» *Risks Digest ,* vol. 22, nº 17, 2002.

[76] S. P. Everett, The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection, Houston, Texas: PhD thesis, Rice University, 2007.

[77] T. Selker y J. Goler, «Security vulnerabilities and problems with VVPAT.,» de *Voting Technology Project*, Pasadena, California, Caltech/MIT, 2004, p. Paper 13.

[78] Compuware Corp, «Direct recording electronic (DRE) technical security assessment report.,» 02 11 2003. [En línea]. Available: http://www.sos.state.oh.us/sos/upload/everest/01-compuware112103.pdf . [Último acceso: 07 07 2013].

[79] A. Rubin, «avi-rubin.blogspot.com,» 07 03 2007. [En línea]. Available: http://avi-rubin.blogspot.com.es/2007/03/todays-congressional-hearing.html. [Último acceso: 08 09 2013].

[80] M. I. Shamos, «NIST-Threats,» 5 10 2005. [En línea]. Available: http://www.bbvdocs.org/reports/NIST-Threats/papertrailhack.pdf. [Último acceso: 08 09 2013].

[81] T. Hommel, «http://www.uuvv.org,» 26 05 2009. [En línea]. Available: http://www.uuvv.org/VVPAT_Idea_Failed.pdf. [Último acceso: 28 01 2014].

[82] B. Adida y R. L. Rivest, «Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting,» de *ACM Workshop on Privacy in the Electonic Society*, ACM, 2006, pp. 29-35.

[83] P. Paillier, «Public-key cryptosystems based on composite degree residuosity classes,» de *Lecture Notes in Computer Science.Volume 1592*, Springer, 1999, p. 223–238.

[84] O. Baudron y et al., «Practical multi-candidate election system,» *PODC de ACM,* pp. 274-283, 2001.

[85] Verified Voting Foundation, «Verified Voting Foundation website,» 24 09 2009. [En línea]. Available: http://verifiedvotingfoundation.net. [Último acceso: 13 07 2013].

[86] R. Mercuri, «A better ballot box?,» *IEEE Spectrum,* vol. 10, nº 39, pp. 46-50, 2002.

[87] Brennan Centre for Justice and Leadership Conference on Civil Rights, «brennancenter.org,» 01 07 2004. [En línea]. Available: http://www.brennancenter.org/publication/recommendations-improving-reliability-direct-recording-electronic-voting-systems. [Último acceso: 07 07 2013].

[88] D. W. Jones, «Auditing elections.,» *Communications of the ACM,* vol. 47, nº 10, pp. 46-50, 2004.

[89] N. Lawrence, A. Burstein, J. L. Hall y M. Chen, «Post-election audits: Restoring trust in elections. Technical report, Brennan Center for Justice,» 09 08 2007. [En línea]. Available: http://www.brennancenter.org/page/-/d/download_file_50228.pdf. [Último acceso: 13 07 2013].

[90] V. M. Morales , Seguridad en los procesos de voto electrónico remoto: registro, votación, consolidación de resultados y auditoria, Barcelona, España: Tesis doctoral Universidad Politécnica de Cataluña, 2009.

[91] J. A. Calandrino, J. A. Halderman y E. W. Felten, «Machine-assiste delection auditing,» de *EVT'07, the USENIX/ACCURATE Electronic Voting Tech .Workshop.* , Boston, 2007.

[92] A. D. Rubin, Brave New Ballot, New York: Morgan Road Books, 2006.

[93] C. d. G. (Suiza), «www.geneve.ch,» [En línea]. Available: www.geneve.ch/evoting. [Último acceso: 15 10 2014].

[94] Cantón de Geneva, Suiza, «E-voting–Internet voting in Geneva, frequently asked questions (faq).,» 2009. [En línea]. Available: http://www.ge.ch/evoting/faq/vote-internet/. [Último acceso: 13 07 2013].

[95] D. e. d. Bélgica, «www.ibz.rrn.fgov.be,» [En línea]. Available: www.ibz.rrn.fgov.be/index.php?id=3285&L=0#. [Último acceso: 15 10 2014].

[96] Organization for Security and Cooperation in Europe, « Expert vision new voting technologies : 8 October 2006 local elections, Kingdom of Belgium. Technical Report ODIHR22450,» 22 11 2006. [En línea]. Available: http://www.osce.org/odihr/elections/22450. [Último acceso: 13 07 2013].

[97] Election Process Advisory Commission (Holanda), «http://wijvertrouwenstemcomputersniet.nl,» 2007. [En línea]. Available: http://wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf. [Último acceso: 15 10 2014].

[98] B. Fairweather y S. Rogerson, «The implementation of electronic voting in the UK technical options report,» 02 05 2002. [En línea]. Available: http://dematerialisedid.com/PDFs/tech-report.pdf . [Último acceso: 07 07 2013].

[99] Comisión electoral de Reino Unido, «http://www.electoralcommission.org.uk,» [En línea]. Available: http://www.electoralcommission.org.uk. [Último acceso: 15 10 2014].

[100] Parlamento Escocés, «http://www.scottish.parliament.uk,» [En línea]. Available: http://www.scottish.parliament.uk/gettinginvolved/petitions/. [Último acceso: 03 12 2013].

[101] IRISH CITIZENS FOR TRUSTWORTHY E-VOTING, «http://www.stdlib.net,» [En línea]. Available: http://www.stdlib.net/~colmmacc/letter-to-pubcom-2.pdf. [Último acceso: 15 10 2014].

[102] Digital Civil Rights in Europe, «http://history.edri.org/,» [En línea]. Available: http://history.edri.org/edri-gram/number7.5/no-evoting-germany. [Último acceso: 15 10 2014].

[103] A. Prosser, R. Kofler y et al., «http://epub.wu.ac.at,» [En línea]. Available: http://epub.wu.ac.at/194/. [Último acceso: 15 10 2014].

[104] Standford University, «cs.stanford.edu,» 2007. [En línea]. Available: http://cs.stanford.edu/people/eroberts/cs201/projects/2006-07/electronic-voting/index_files/page0005.html. [Último acceso: 15 10 2014].

[105] Central Election Commission of the Russian Federation, «http://www.cikrf.ru/eng/,» [En línea]. Available: http://www.cikrf.ru/eng/. [Último acceso: 15 10 2014].

[106] Johns Hopkins University, «http://isi.jhu.edu/,» Johns Hopkins University, [En línea]. Available: http://isi.jhu.edu/. [Último acceso: 03 12 2013].

[107] National Science Foundation , «http://www.nsf.gov/,» NSF, [En línea]. Available: http://www.nsf.gov/. [Último acceso: 03 12 2013].

[108] Department of Justice, «http://www.justice.gov/,» justice.gov, [En línea]. Available: http://www.justice.gov/crt/about/vot/hava/hava.php.

[109] A. D. Rubin, «Can a voting machine that is rigged for a particular candidate pass certification?,» 02 04 2004. [En línea]. Available: www.docstoc.com/docs/35183638/Can-a-Voting-Machine-that-is-Rigged-for-a-Particular-Candidate. [Último acceso: 07 07 2013].

[110] Centro Carter, «http://www.cartercenter.org,» 07 2006. [En línea]. Available: http://www.cartercenter.org/resources/pdfs/peace/americas/EstudioElectoralVenezuela1%20CarterCenter.pdf. [Último acceso: 18 10 2014].

[111] Foundation Open Society Institute, «www.ibanet.org,» 06 2007. [En línea]. Available: www.ibanet.org%2FDocument%2FDefault.aspx%3FDocumentUid%3D41f4c43b-b545-4682-ae64-43b51295d5e3&ei=fv9DVMyIK87TaKTTgtAE&usg=AFQjCNGfzGk8CFucmHkIFd7qVnPSKnWllw. [Último acceso: 18 10 2014].

[112] Ciencias y cosas, «http://cienciasycosas.wordpress.com,» wordpress.com, [En línea]. Available: http://cienciasycosas.wordpress.com/2013/01/06/el-fraude-del-voto-electronico-en-las-elecciones-de-rio-do-janeiro/. [Último acceso: 03 12 2013].

[113] Indian EVM, «http://www.indianevm.com/,» [En línea]. Available: http://www.indianevm.com/. [Último acceso: 18 10 2014].

[114] Electoral Council of Australia and New Zealand, «http://www.elections.wa.gov.au,» 10 09 2013. [En línea]. Available: http://www.elections.wa.gov.au/sites/default/files/content/documents/ECANZ_Internet_Voting_Aus.pdf. [Último acceso: 18 10 2014].

[115] Concil of Europe, «http://www.coe.int,» 25 03 2004. [En línea]. Available: http://www.coe.int/t/dgap/democracy/activities/GGIS/E-voting/Work_of_e-voting_committee/02_Agendas_and_Reports/49IP1(2004)30_Report_Las_Palmas_en.asp. [Último acceso: 28 11 2013].

[116] COUNCIL OF EUROPE. COMMITTEE OF MINISTERS, «https://wcd.coe.int,» 30 09 2004. [En línea]. Available: https://wcd.coe.int/ViewDoc.jsp?id=778189. [Último acceso: 28 11 2013].

[117] J. Barrat, «http://www.idea.int/,» Idea, [En línea]. Available: http://www.idea.int/democracydialog/upload/Observing-e-enabled-elections-how-to-implement-regional-electoral-standards.pdf. [Último acceso: 03 12 2013].

[118] D. W. Jones, «The European 2004 draft e-voting standard: Some critical comments.,» 11 10 2004. [En línea]. Available: http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml. [Último acceso: 13 07 2013].

[119] Council of Europe Publishing, «E-voting handbook,» 02 11 2010. [En línea]. Available: http://www.coe.int/t/dgap/democracy/Activities/GGIS/E-voting/E-voting%202010/Biennial_Nov_meeting/ID10322%20GBR%206948%20Evoting%20handbook%20A5%20HD.pdf. [Último acceso: 13 07 2013].

[120] Scytl, «http://www.scytl.com,» scytl.com, [En línea]. Available: http://www.scytl.com. [Último acceso: 03 12 2013].

[121] Indra, «indracompany.com,» Indra, [En línea]. Available: http://www.indracompany.com/soluciones-y-servicios/solucion/Procesos%20Electorales. [Último acceso: 04 12 2013].

[122] J. Carracedo, A. Gómez, E. Pérez, J. Moreno y J. D. Carracedo, Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT), Mérida, Venezuela, 2002.

[123] Ayuntamiento de Jun, «http://www.ayuntamientojun.org,» ayuntamientojun.org, [En línea]. Available: http://www.ayuntamientojun.org/cedj. [Último acceso: 03 12 2013].

[124] Observatorio del voto electrónico, «http://www.votobit.org,» votobit.org, [En línea]. Available: http://www.votobit.org/misiones/pruebas/informes.html. [Último acceso: 03 12 2013].

[125] La Vanguardia, «http://www.lavanguardia.com,» lavanguardia.com, [En línea]. Available: http://www.lavanguardia.com/vida/20100516/53928946995/el-fracaso-de-la-consulta-de-la-diagonal-se-lleva-por-delante-al-primer-teniente-de-alcalde.html. [Último acceso: 03 12 2013].

[126] El Confidencial, «http://www.elconfidencial.com,» elconfidencial.com, [En línea]. Available: http://www.elconfidencial.com/espana/2011/policia-ministerio-del-interior-telefonica-20110705-80985.html. [Último acceso: 03 12 2013].

[127] IST World, «CYBERVOTE - An innovative cyber voting system for Internet terminals and mobile phones,» 31 03 2003. [En línea]. Available: http://www.ist-world.org/ProjectDetails.aspx?ProjectId=019ccb17d33e4be4b341e8270d7785f6&SourceDatabaseId=9cd97ac2e51045e39c2ad6b86dce1ac2. [Último acceso: 19 10 2014].

[128] D. Jefferson, A. D. Rubin y et al, «Analyzing Internet Voting Security.,» *Communications of the ACM,* vol. 47, nº 10, pp. 59-64, 2004.

[129] Gobierno de Estonia, «http://www.vvk.ee,» vvk.ee, [En línea]. Available: http://www.vvk.ee/voting-methods-in-estonia/engindex. [Último acceso: 04 12 2013].

[130] G. d. Estonia, «https://estoniaevoting.org,» [En línea]. Available: https://estoniaevoting.org. [Último acceso: 03 03 2014].

[131] J. Barrat i Esteve, B. Goldsmith y J. Turner, «International Experience with E-voting. Norwegian E-vote project,» 01 06 2012. [En línea]. Available: http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf . [Último acceso: 13 07 2013].

[132] Norwegian Ministry of Local Government and Regional Development, «11 municipalities to try out e-voting in 2011,» 27 01 2010. [En línea]. Available: http://www.regjeringen.no/nb/dep/krd/prosjekter/e-valg-2011-prosjektet/evaluering/evalueringen-av-e-valgforsoket-er-tilgje.html?id=684642. [Último acceso: 13 07 2013].

[133] International Council on Korean Studies (ICKS), «www.icks.org,» [En línea]. Available: http://www.icks.org/publication/pdf_2005_s/5_Lee.pdf. [Último acceso: 19 10 2014].

[134] Electronic Frontier Finland – Effi, «www.verifiedvoting.org,» 28 11 2009. [En línea]. Available: https://www.verifiedvoting.org/wp-content/uploads/2014/09/Finland-2008-EFFI-Report.pdf. [Último acceso: 19 10 2014].

[135] D. Jefferson, A. D. Rubin, B. Simons y D. Wagner, «A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE).,» 20 01 2004. [En línea]. Available: http://www.servesecurityreport.org/. [Último acceso: 21 5 2013].

[136] Serve security report, «http://www.servesecurityreport.org/,» servesecurityreport.org, [En línea]. Available: http://www.servesecurityreport.org/. [Último acceso: 03 12 2013].

[137] B. Adida, «Helios: web-based open-audit voting,» *Proceedings of the 17th conference on Security symposium,* vol. 1, nº 8, pp. 335-348, 2008.

[138] Observatorio del voto electrónico, «http://www.votobit.org/,» votobit.org, [En línea]. Available: http://www.votobit.org/misiones/pruebas/2m6.html. [Último acceso: 03 12 2013].

[139] D. Chaum, «Untraceable electronic mail, return addresses, and digital pseudonyms,» *Magazine Communications of the ACM,* vol. 24, nº 2, pp. 84-90, 1981.

[140] R. A. Fink, Applying Trustworthy Computing to End-To-End Electronic Voting (Thesis), Baltimore: University of Maryland, Baltimore County, 2010.

[141] R. A. Fink y A. Sherman, «Combining end-to-end voting with trustworthy computing for greater privacy, trust, accessibility, and usability (summary),» *Proceedings of the National Institutes of Technology (NIST) workshop on end-to-end voting systems,* 2009.

[142] S. Popoveniuc, J. M. Kelsey, A. R. Regenscheid y P. Vora, «Performance Requirements for End-to-End Verifiable Elections,» de *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE '10)*, Washington, DC, 2010.

[143] R. T. Carback III, Engineering Practical End-to-End Verifiable Voting Systems (Thesis), Baltimore: University of Maryland, Baltimore County (UMBC), 2010.

[144] D. W. Jones, «Some problems with End-to-End Voting,» de *NIST Workshop on End-to-End Voting Systems, Oct. 14, 2009,*, Washington DC., 2009.

[145] D. W. Jones, «Some Problems with End-to-End Voting,» [En línea]. Available: http://csrc.nist.gov/groups/ST/e2evoting/documents/papers/Jones_E2E_Paper.pdf. [Último acceso: 26 01 2014].

[146] A. Essex, J. Clark, R. T. I. Carback y S. Popoveniuc, «http://punchscan.org,» [En línea]. Available: http://punchscan.org/vocomp/PunchscanVocompSubmission.pdf. [Último acceso: 26 01 2014].

[147] D. Chaum, R. Carback, S. Popoveniuc, R. L. Rivest y P. Y. Ryan, «Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes,» 2008. [En línea]. Available: https://www.usenix.org/legacy/event/evt08/tech/full_papers/chaum/chaum.pdf. [Último acceso: 29 01 2014].

[148] R. L. Rivest, «The ThreeBallot Voting System,» 1 10 2006. [En línea]. Available: http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf. [Último acceso: 26 11 2013].

[149] B. Adida y R. L. Rivest, «Scratch & Vote. Self-Contained Paper-Based Cryptographic Voting,» *WPES'06,* vol. October, pp. 29-35, 2006.

[150] P. Y. A. Ryan, D. Bismark, J. Heather y S. Schneider, «Prêt à Voter: a Voter-Verifiable Voting System,» *Information Forensics and Security,* vol. 4, nº 4, pp. 662 - 673, 2009.

[151] J. M. Bohli, J. Müller-Quade y S. Röhrich, «Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator,» *VOTE-ID 2007, LNCS 4896,* pp. 111-124, 2007.

[152] Helios Voting, «heliosvoting.org,» Helios Voting, [En línea]. Available: https://vote.heliosvoting.org/. [Último acceso: 03 12 2013].

[153] J. Benaloh, «Simple verifiable elections,» *EVT'06 Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop ,* pp. 5-5, 2006.

[154] Adder, «(http://cryptodrm.engr.uconn.edu/adder/index.shtml),» [En línea]. Available: (http://cryptodrm.engr.uconn.edu/adder/index.shtml). [Último acceso: 03 03 2014].

[155] A. Kiayias, M. Korman y D. Walluck, «An Internet Voting System Supporting User Privacy,» *Computer Security Applications Conference,* vol. 22, nº 1, pp. 165 - 174, 2006.

[156] J. E. Gilbert, «primevotingsystem.org/,» [En línea]. Available: http://www.primevotingsystem.org/. [Último acceso: 07 06 2014].

[157] D. Chaum y R. Carback, «http://www.punchscan.org/,» 2006. [En línea]. Available: http://www.punchscan.org/. [Último acceso: 29 01 2014].

[158] D. Chaum, «Secret-ballot receipts: True voter-verifiable elections.,» *Security and Privacy,* pp. 38-47, 2004.

[159] Vocomp, «http://www.vocomp.org,» [En línea]. Available: http://www.vocomp.org. [Último acceso: 03 03 2013].

[160] R. T. Carback III, J. Clark, A. Essex y S. Popoveniuc, «http://users.encs.concordia.ca,» 2007. [En línea]. Available: http://users.encs.concordia.ca/~clark/papers/2007_vocomp_paper.pdf. [Último acceso: 05 03 2014].

[161] S. Popoveniuc y B. Hosp, «popoveniuc.com,» 01 06 2010. [En línea]. Available: http://popoveniuc.com/papers/PunchScan.pdf. [Último acceso: 25 02 2014].

[162] S. Popoveniuc y B. Hosp, «An Introduction to PunchScan,» de *Towards Trustworthy Elections. Lecture Notes in Computer Science Volume 6000*, Berlin, Springer Berlin Heidelberg, 2010, pp. 242-259.

[163] Punchscan, «http://www.punchscan.org/elections.php.html,» [En línea]. Available: http://www.punchscan.org/elections.php.html. [Último acceso: 03 03 2013].

[164] K. Fisher, R. Carback y A. Sherman, «Punchscan: Introduction and System Definition of a High-Integrity Election System,» *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE 2006),* 2006.

[165] A. T. Sherman, R. A. Fink, R. Carback y D. Chaum, «Scantegrity III: automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability,» *EVT/WOTE'11 Proceedings of the 2011 conference on Electronic voting technology/workshop on trustworthy elections,* pp. 7-7, 2011.

[166] R. Carback, D. Chaum, J. Clark y et al., «Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy,» *USENIX Security'10 Proceedings of the 19th USENIX conference on Security,* pp. 19-19, 2010.

[167] Scantegrity, «Elecciones con Scantegrity,» [En línea]. Available: http://scantegrity.org/elections.php. [Último acceso: 03 03 2013].

[168] California Institute of Technology, «http://caltech.edu/,» 18 12 2006. [En línea]. Available: http://electionupdates.caltech.edu/2006/12/18/threeballot-tested-by-mit-students/. [Último acceso: 29 01 2014].

[169] O. d. Marneffe, O. Pereira y J. J. Quisquater, «Simulation-Based Analisys of E2E Voting Systems,» *VOTE-ID 2007 (LNCS 4896),* pp. 137-149, 2007.

[170] A. W. Appel, «How to defeat Rivest's ThreeBallot Voting System,» 05 10 2006. [En línea]. Available: http://www.cs.princeton.edu/~appel/papers/DefeatingThreeBallot.pdf. [Último acceso: 29 01 2014].

[171] K. Henry, D. R. Stinson y S. Jiayuan, «The Effectiveness of Receipt-Based Attacks on ThreeBallot,» *IEEE Transactions on Information Forensics and Security,* vol. 4, nº 4, pp. 699 - 707, 2009.

[172] R. Araujo, R. F. Custodio y J. Graaf, «A verifiable voting protocol based on farnel,» de *IAVoSS Workshop On Trustworthy Elections*, Ottawa, Canada, 2007.

[173] Prêt á Voter, «pretavoter.com,» 2005. [En línea]. Available: http://www.pretavoter.com/. [Último acceso: 26 03 2014].

[174] P. Y. Ryan, D. Bismark, J. Heather y S. Schneider, «Prêt à Voter: a Voter-Verifiable Voting System,» *Information Forensics and Security,* vol. 4, nº 4, pp. 662 - 673, 2009.

[175] D. Chaum, P. Y. A. Ryan y S. Schneider, «A practical voter-verifiable election scheme,» *Proceedings of the 10th European conference on Research in Computer Security,* vol. 1, nº 1, pp. 118-139, 2005.

[176] D. Bismark, J. Heather, R. M. A. Peel, S. Schneider y P. Y. Ryan, «Experiences Gained from the first Prêt à Voter Implementation,» *Requirements Engineering for e-Voting Systems (RE-VOTE),* vol. 1, nº 1, pp. 19-28, 2009.

[177] Trustworthy Voting Systems, «http://www.tvsproject.org/,» [En línea]. Available: http://www.tvsproject.org/ . [Último acceso: 05 04 2013].

[178] M. Winckler, R. Bernhaupt, P. Palanque y et al., «Assessing the Usability of Open Verifiable e-Voting Systems.,» de *Proceedings of the 1st International Conference on eGovernment and eGovernnace (ICEGOV).*, Ankara, Turquía., 2009.

[179] C. Henrich, «Institut für Kryptographie und Sicherheit (IKS),» 2012. [En línea]. Available: http://digbib.ubka.uni-karlsruhe.de/volltexte/1000030270. [Último acceso: 07 02 2014].

[180] Project Bingo Voting, «https://crypto.iti.kit.edu,» [En línea]. Available: https://crypto.iti.kit.edu/index.php?id=project-bingovoting. [Último acceso: 05 04 2013].

[181] J. Kelsey, A. Regenscheid, T. Moran y D. Chaum, «Attacking Paper-Based E2E Voting Systems,» de *Towards Trustworthy Elections. New Directions in Electronic Voting*, Berlin, Springer Berlin Heidelberg, 2010, pp. 370-387.

[182] S. Popoveniuc y D. Lundin, «A simple technique for safely using Punchscan and Prêt à Voter in mail-in elections,» *Proceeding VOTE-ID'07 Proceedings of the 1st international conference on E-voting and identity,* pp. 150-155, 2007.

[183] T. Tjøstheim, T. Peacock y P. A. Ryan, «A case study in system-based analysis: The Threeballot voting system and Pret a voter,» de *VoComp*, Portland, Oregon, 2007.

[184] T. Moran y M. Naor, «Split-ballot voting: Everlasting privacy with distributed trust,» *ACM Transactions on Information and System Security (TISSEC),* vol. 13, nº 2, pp. 1-43, 2010.