Votación electrónica y democracia

ALEJANDRO HEVIA

Profesor Asistente del Departamento de Ciencias de la Computación de la Universidad de Chile. Director del Laboratorio de Criptografía Aplicada y Ciberseguridad, CLCERT. Doctor en Computación por la Universidad de California, San Diego. Sus intereses de investigación incluyen criptografía aplicada y seguridad computacional.

ahevia@dcc.uchile.cl

"El derecho a voto es un derecho básico sin el cual todos los otros carecen de sentido. A las personas, a los individuos, les entrega control sobre sus propios destinos". Lyndon B. Johnson.

Introducción

La elección democrática de nuestros representantes es probablemente hoy en día uno de los procesos sociales colectivos más importantes en una sociedad. Debatida, amada y frecuentemente vilipendiada, la elección de representantes requiere de legitimidad, esto es, no solo debe cumplir objetivos como participación ciudadana, facilidad y libertad de ejercer el derecho, sino debe proveer transparencia y confianza. En otras palabras, debe ser convincente. "El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor" habría dicho Dan Wallace, académico de la Universidad de Princeton. La legitimidad entonces debe cumplirse con respecto a todos (o la gran mayoría de) los participantes, tanto los involucrados directamente en el proceso eleccionario como de los que no, dado que su resultado tiene efectos para toda la sociedad.

Alcanzar los objetivos, sin embargo, depende crucialmente del sistema de votación, esto es, el mecanismo o procedimiento, utilizado para lograr la elección. Por ejemplo, un sistema de votación a mano alzada es simple y fácil de usar, pero no escala cuando la comunidad crece. Peor aún, este sistema revela la preferencia individual (el voto) de cada ciudadano, dando pie a posible intimidación y compra de votos, coartando así la libertad de votar por una preferencia. El sistema actual de votación chileno lo hace posiblemente mejor: cada ciudadano toma un papel preimpreso donde aparecen todos los candidatos (denominado la "papeleta australiana") y marca allí su preferencia en forma secreta con un lápiz. Luego, la papeleta es despojada de toda referencia al votante y depositada en una urna, donde se confunde o mezcla con las otras papeletas. El conteo de votos luego se hace en forma pública, abriendo la urna en presencia de participantes que velan por el correcto desarrollo del conteo. El sistema también contempla un paso previo, menos mencionado pero no por eso menos importante: el manejo del registro electoral. Esto incluye tanto la inscripción inicial de los votantes (por el votante cuando es voluntaria, o por la agencia estatal a cargo cuando es obligatorio) así como la mantención del registro (muertes, cambios de domicilio, etc.).

Desafortunadamente, los procesos basados en papel como el chileno son frecuentemente vistos con desdén en una era donde los teléfonos inteligentes están en todos lados e Internet juega un rol central en la vida de las personas. ¿Si podemos usar nuestros computadores para hacer transacciones bancarias, participar remotamente en reuniones, e incluso hacer cirugías médicas en forma segura, por qué no podemos votar usando computadores en forma segura? Como veremos, la respuesta a esta pregunta requiere un análisis más complejo de lo sospechado a primera vista.

El objetivo de un sistema de votación

En principio, un sistema de votación pareciera ser algo simple ¡solo debemos contar! En realidad, un sistema de votación es un proceso complejo por la combinación de requerimientos aparentemente contradictorios que nos demanda. Desde un punto de vista funcional, un sistema de votación debe cumplir los siguientes requisitos:

1. ***Integridad:*** el resultado de la elección debe coincidir con las intenciones de voto de los votantes. Tal requerimiento usualmente se divide en dos condiciones (a) el voto es emitido (registrado) de acuerdo a la preferencia del votante, y (b) los votos son contados considerando las preferencias registradas.

2. ***Secreto del voto:*** nadie puede saber cómo votó un votante. Frecuentemente, se pide incluso algo más fuerte; nadie puede saber cómo votó **aún si el votante** desea revelarlo.

3. ***Autentificación de los votantes:*** solo los votantes autorizados pueden emitir votos, pero cada votante puede hacerlo solo una vez.

4. ***Derecho a voto:*** todas las personas autorizadas tienen la oportunidad de votar.

5. ***Disponibilidad:*** el sistema de votación debe ser capaz de (a) aceptar todos los votos emitidos durante un periodo pre-especificado, y (b) producir resultados razonables después de un periodo razonable.

Diseñar sistemas de votación es complejo pues los requerimientos anteriores están en tensión: por ejemplo, la integridad del sistema y la privacidad de los votos[1], o la autentificación de los votantes con el derecho a voto.

Peor aún, todo sistema de votación no ocurre en un ambiente ideal, con ciudadanos ejemplares y candidatos honestos. Un sistema de votación es usado para una elección concreta, la cual tiene amenazas, personas y entidades (adversarios) que desean atacar o usar el siste-

1 | Por ejemplo, la votación a mano alzada es obviamente correcta pero no privada.

Figura 1. "La Elección en el Condado, 1852", G.C. Bingham, pintor norteamericano 1811–1879; Museo de Arte de Saint Louis. Muestra la naturaleza caótica de una elección en 1800, incluyendo acarreos y compra de votos en un proceso a viva voz.

Fuente: Wikipedia, dominio público.

ma en su beneficio. Candidatos que desean ganar a toda costa, o sus mismos votantes quienes pueden querer alterar los votos de otros o vender sus propios votos, funcionarios encargados de ejecutar el sistema pero excesivamente politizados que pueden desear ver ganador a un cierto candidato, los fabricantes de algunas de las partes tecnológicas del sistema utilizado, o incluso potencias extranjeras posiblemente afectadas por el resultado que desean manipularlo o desacreditarlo (ver Figura 1).

El tipo de amenazas es crucial para evaluar un sistema de votación. Una elección gremial, o estudiantil pequeña, es considerada de "bajo perfil" puesto que quien gane o pierda es poco relevante para actores poderosos que pudieran montar ataques significativos. Probablemente pueda llevarse a cabo en forma segura utilizando un sistema de votación relativamente simple.

La efectividad y severidad de los ataques que reciba estarán acotados, simplemente porque las amenazas serán pequeñas: tanto los candidatos, como los votantes o incluso observadores externos serán probablemente poco sofisticados o tendrán financiamiento limitado, por lo que explorarán maneras simples de alterar la votación. Una elección de "alto perfil" cambia necesariamente esta dinámica. Tal elección sería, por ejemplo, una de nivel nacional, del tipo presidencial o parlamentaria, o incluso local pero significativa, como la de alcaldes. En tal tipo de elección, el sistema de votación debe resistir amenazas más potentes y complejas, esto es, ataques de adversarios mejor financiados, técnicamente más hábiles, y de escala mayor.

¿En qué consiste la votación electrónica?

En general, un sistema de votación electrónica es un sistema de elecciones que utiliza un computador en forma sustantiva en alguna de sus fases. Ahora bien, hoy por hoy, todos los sistemas involucran algún sistema computacional[2] así que es necesario precisar nuestra definición. Llamaremos votación electrónica a todo sistema donde computadores son utilizados en forma exclusiva en algún paso de la votación, ya sea en el proceso de capturar una preferencia ("votar" o transformar una preferencia mental en una marca en una papeleta) o en el proceso de transmitir o contar los votos, descartando el proceso de registro.

Los sistemas de votación mecánicos existen desde fines de 1800. Sistemas basados en procesos mecánicos con palancas y engranajes *(lever machines)*, y en papel perforado manualmente *(punch-card systems)* siguieron en uso hasta inicios de este siglo, siendo populares en Estados Unidos. Los sistemas propiamente electrónicos basados en componentes computacionales comenzaron a usarse en la década de 1960 en la forma de escáners para leer formularios llenados manualmente. Recién en la década de 1970 surgen los primeros computadores utilizados para registrar y contabilizar los votos.

Una primera distinción: remota versus presencial

Frecuentemente el ciudadano común entiende por "votación electrónica" a la votación remota, esto es, al sistema donde emitir el voto es hecho en computador pero en forma remota respecto

2 | En Chile, por ejemplo, el sistema de registro de votantes y el sistema de recopilación preliminar de conteos utilizan computadores.

Figura 2. Escáner usado para leer papeletas de votación en la forma de formularios.

Fuente: Wikipedia.

Figura 3. Computador marcador de papeletas: solicita las preferencias al usuario y luego las imprime en una papeleta de votación.

Fuente: Wikipedia.

Figura 4. Máquina de tipo DRE usada en Estados Unidos.

Fuente: Verified Voting Foundation.

al lugar donde se cuentan los votos, y donde la transmisión de las papeletas con las preferencias registradas es hecha por una red computacional. En otras palabras, votar en un computador o teléfono inteligente en la casa. Si esta red es Internet, hablaremos de votación por Internet.

La votación electrónica puede ser también presencial *(pollsite)* sin embargo. Esto es, puede ocurrir en un recinto de votación físicamente protegido y monitoreado al cual los votantes acceden en persona, y donde el computador ayuda al votante ya sea a emitir y/o contar los votos. Discutiremos este tipo, históricamente más antiguo, a continuación.

Los inicios de la votación electrónica

La variante más antigua de votación usando computadores tal como los entendemos hoy, toma la forma de escáners. En ella, los votantes llenan (usualmente en forma manual) una papeleta con sus preferencias o votos. Esta papeleta, denominada *"optical-scan ballots"*, toma la forma de un formulario legible por un computador, por ejemplo, con óvalos en blanco como los utilizados en las pruebas de selección universitaria. Luego, un computador (un escáner) utiliza una cámara para leerlas ópticamente, calculando el conteo o almacenando localmente los totales parciales (ver Figura 2). Con la llegada de interfaces gráficas y táctiles, los computadores también empezaron a ser usados para interactuar con el votante, obtener sus preferencias y permitirle más fácilmente producir (imprimir) la papeleta llena, previo al conteo (ver Figura 3).

En retrospectiva, los computadores pasaron desde ser usados solo para contar papeletas (calcular el total), a ser usados también para generar las papeletas completas. No es sorprendente que el siguiente paso fuera hacer ambos simultáneamente, sin imprimir la papeleta. La máquina de "Captura y almacenamiento electrónico directo", o DRE por su sigla en Inglés (Direct-Recording Electronic machine) es posiblemente la implementación más directa de un sistema de votación electrónico usando íntegramente un computador (ver Figura 4). Frecuentemente usando una interfaz gráfica, el DRE despliega opciones o candidatos desde donde el votante escoge sus preferencias. En teoría, su selección es registrada y almacenada en forma interna, en memoria o disco. Al finalizar la elección, el conteo puede realizarse en el mismo DRE y/o la información de los votos o totales transmitirse a un servidor central. La transmisión puede hacerse vía tarjetas de memoria, USB, o incluso utilizando una red computacional.

Los sistemas DRE siguen siendo muy populares en Estados Unidos y en el mundo pese a las dificultades que mencionaremos a continuación.

Muchos ataques y pocas defensas

"Lo que realmente cuenta no son las personas que votan, sino las personas que cuentan los votos". Atribuido a José Stalin.

¿Cómo sabemos si un sistema es seguro? Intuitivamente, debe cumplir los requerimientos mencionados anteriormente. Claramente, si existe un ataque que viola alguno de ellos, no es seguro.

Existen ataques documentados a varios sistemas basados en escáners donde el total puede ser manipulado si el atacante llegara a tener acceso limitado a los escáners [Kiayas et al. 2006]. Pese a estas noticias, en la práctica los sistemas basados en escaneadores son, entre todos los sistemas que utilizan computadores, probablemente los más fáciles de "segurizar" hoy en día. Basta notar que

su operación produce naturalmente una traza verificable en papel (esto es, el formulario lleno) cuya correctitud puede ser verificada directamente por el votante en forma manual antes de ser contada por el computador. Suponiendo un manejo adecuadamente seguro de las papeletas, cualquier problema es corregible; basta recontar las papeletas. Lamentablemente, en la práctica no siempre es posible, como observaremos luego.

En general, la seguridad de los dispositivos DRE ha sido paupérrima. Desde inicios del 2000, los ataques documentados a estos sistemas han sido numerosos y devastadores. Por ejemplo, investigadores de Princeton en 2006 mostraron serios ataques al sistema "Diebold Accuvote TS". Un votante con un breve acceso físico a la máquina era capaz de alterar el programa de la máquina cambiando los totales en forma indetectable. Peor aún, el atacante podría crear un virus (malware) capaz de infectar otras máquinas y el sistema de conteo central [Feldman et al. 2006]. Diversos otros ataques han sido documentados para sistemas similares, desde violación del secreto del voto vía emanaciones electromagnéticas de un sistema en Holanda [Gonggrijp et al. 2007] hasta instalar juegos en el sistema (DEFCON hacking village 2018).

Diseñar sistemas DRE seguros ha resultado extremadamente difícil aún si son simples. Ejemplo de ellos son los sistemas usados en Brasil desde 1996, del tipo DRE, muy simples usando tarjetas de memoria para almacenar los votos (ver Figura 5). Un estudio académico mostró que el total podía ser alterable por un votante malicioso, y que, peor aún, los registros públicos podían filtrar el voto de cada ciudadano, solo conociendo la hora de inicio de la votación [Aranha et al. 2019]. El sistema DRE usado en la India en forma nacional desde de 2004 fue diseñado para ser aún más básico, sin pantalla y con una interfaz simple consistente en botones (ver Figura 6). Pese a que el conteo se realiza en el mismo dispositivo al finalizar la elección, se mostró que eran susceptible a ataques similares a los descritos anteriormente [Wolchok et al. 2010].

La deficiencia principal de los sistemas DRE es su opacidad. Sin mecanismos para garantizar que el conteo es realizado correctamente, cuando dicho conteo se realiza en forma interna y los registros de los votos se mantienen en forma digital, ¿cómo puede un observador externo verificar a ciencia cierta que el total fue calculado correctamente? ¿Cómo puede un votante asegurarse que el computador no viola la privacidad del voto llevando un registro subrepticio de cómo han votado los ciudadanos? La clave aquí es la ausencia de evidencia convincente, comprobable por externos, que el resultado es correcto. Esta evidencia debe ser compatible con el secreto del voto, y con el requerimiento de confiar lo menos posible en la menor cantidad de entidades posibles, dado que cualquier participante es potencialmente un adversario.

Una estrategia para mitigar la inseguridad de los sistemas DRE consiste en extenderlos con un mecanismo para imprimir trazas en papel verificables por el votante (VVPAT, por su nombre en inglés) (ver Figura 7). Cada votante puede verificar que su preferencia ha sido correctamente capturada al menos en una copia en papel de su voto, permitiendo una contabilidad basada en las papeletas físicas en caso de cuestionamiento. Desafortunadamente, esta posibilidad de recuento puede no concretarse nunca si se carece de procedimientos y/o legislación que garantice la preservación de dichas papeletas y permita a los ciudadanos solicitar su revisión y conteo posterior bajo condiciones razonables. En varios estados de Estados Unidos, en las elecciones de 2016, y pese a utilizar sistemas con VVPAT en muchos estados, intentos de recuento fueron obstaculizados y negados administrativa y legalmente, inutilizando los VVPATs como mecanismo de verificación en la práctica.

En caso de tener respaldo legal y administrativo robusto, los procedimientos de auditoría estadística denominados *Risk Limiting Audits* (RLA) permiten determinar, con alta probabilidad, si el resultado publicado es consistente con el registro auditable (VVPAT o similar). La operación consiste en seleccionar aleatoriamente un subconjunto pequeño de las papeletas emitidas y recontarlas (o compararlas) para garantizar la correctitud del resultado de la elección. Sin embargo, como lo demuestra la experiencia en Estados Unidos, este proceso debe ser la norma y no la excepción. La recomendación actual de la Academia Nacional de Ciencias, Ingeniería y Matemática (NASEM) de los Estados Unidos es de hecho incluir estrategias de verificación estadística como los RLAs en todos los proyectos de sistemas de

Figura 5. Urna de tipo DRE usada en las elecciones de Brasil en 2005.

Fuente: Wikipedia.

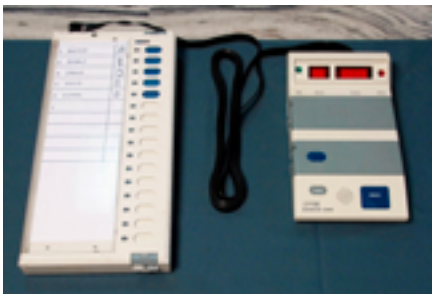

Figura 6. Máquina de votación utilizada en la India.

Fuente: Wikipedia.

Figura 7. Máquina DRE con VVPAT. La ventana de plástico transparente (a la izquierda en la foto) muestra la papeleta impresa completa para su aprobación por el votante.

Fuente: Verifiable Voting Foundation.

votación para los próximos diez años, partiendo con proyectos pilotos con miras a una implementación masiva, en elecciones de escala nacional [NASEM 5.7,5.8]. Asimismo, recomienda descontinuar sistemas que NO proveen papel legible por humanos [NASEM 4.11].

Votación remota y sus dificultades

Si la experiencia muestra que los sistemas de votación presenciales han sido difíciles de implementar correctamente, implementar votación remota pareciera ser un desafío de otro planeta. Con la tecnología actual, no sabemos realmente cómo diseñar un sistema de votación remoto seguro, siempre que el sistema use computadores o dispositivos móviles de propósito general. De hecho, es probable que "votar desde el teléfono" sea inherentemente inseguro. La razón es simple: tal sistema debe poder garantizar que la preferencia del votante es capturada correctamente aún si existe software malicioso (malware) en el teléfono o computador del votante. A priori, nada impide crear malware que pueda intervenir el software que registra el voto, mostrando el mensaje "Usted votó por Candidato A" cuando por detrás registra el voto por "Candidato B", una clara violación a la integridad de la elección. Peor aún, el malware conocería la preferencia del votante, violando el secreto del voto. Argumentar que para una cierta versión del sistema operativo o teléfono "no existe malware" es no entender el problema, ignorando los incentivos detrás de todo ataque. Si la elección es de alto perfil e importante, alguien creará tal malware.

Una posible estrategia para soslayar el problema anterior es disponer de un dispositivo cerrado, solo creado y configurado para permitirle al votante emitir su voto. Lograrlo no sería fácil, eso sí. El costo de proveer tal hardware para todos los votantes probablemente sería estratosférico. Además, si la historia reciente nos sirve de guía, desarrollar y mantener en forma transparente un software confiable (seguro y transparente) para dicho dispositivo parece ser una tarea impracticable, aún para gigantes tecnológicos.

Aún dejando de lado ambos problemas anteriores, hay asuntos más delicados que complotarían con esta solución: hoy no sabemos cómo evitar la coerción y venta de votos en un sistema remoto. Simplemente no sabemos cómo excluir los votos emitidos bajo presión en forma remota, cuando alguien le "mira sobre el hombro" o con "una pistola en la cabeza", y en situaciones donde el votante podría estar monitoreado en todo momento. Tampoco es claro qué hacer cuando el votante mismo puede querer vender su voto (por ejemplo haciendo *streaming* de la selección de su preferencia "en vivo"). Algunas sugerencias, como permitir un voto sustitutivo en persona (que un nuevo voto reemplace cualquier voto anterior del mismo votante) al final del periodo de votación pueden paliar parcialmente el problema de coerción, pero no eliminarlo. El robo o venta de credenciales siguen siendo amenazas reales en muchos escenarios de votación remota propuestos. De hecho, el problema de la venta de votos pareciera, hasta donde sabemos, insalvable en estas condiciones.

La dificultad del voto por Internet es al menos igual (sino mayor) pues el carácter abierto de la red introduce una preocupación más pedestre pero significativamente más grave: la posibilidad del "hackeo" remoto. Ataques computacionales basados en explotar vulnerabilidades en los protocolos de red o en la implementación del sistema pudieran comprometer la integridad del total.[3] Si dichos ataques son difíciles de mitigar ya en sistemas informáticos más simples, ¿seremos capaces de mitigarlos apropiadamente en sistemas de votación con requerimientos sustancialmente más complejos? El problema no es el ataque en sí, sino la escala de su impacto: el costo de cambiar 1 voto es probablemente similar al costo de cambiar millones de votos.

El uso de Internet también introduce un nuevo riesgo, la denegación de servicio (DoS). Si bien cualquier sistema

3 | Un ejemplo notable es el ataque al sistema de votación de Washington D.C. en Estados Unidos en 2010 por un equipo de investigadores universitarios los cuales, luego de comprometer totalmente el sistema, solo fueron detectados cuando pusieron el himno de su universidad a todo quien votara [Wolchok et al. 2012].

"El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor". Dan Wallace respecto del rol de la transparencia de los procesos de elección democrática.

conectado a Internet está expuesto a tal ataque, los procesos eleccionarios son extremadamente sensibles a fallas focalizadas. Por ejemplo, un DoS focalizado en una región específica del país con una historia particular de preferencias políticas podría afectar seriamente una elección. Hasta el día de hoy, los ataques DoS focalizados como éste siguen siendo una amenaza sin resolver para estos sistemas.

Un caso relevante de votación por Internet es el caso de Estonia. Usando una tarjeta inteligente, su tarjeta nacional de identidad, los ciudadanos pueden votar remotamente, por Internet, desde 2005. El sistema también implementa una variante del voto sustitutivo para mitigar la coerción. Pese a ser considerado un caso ejemplar de digitalización de servicios, su empleo de Internet y su falta de transparencia, lo ha hecho el blanco de críticas. Un análisis hecho por un grupo independiente de expertos internacionales en 2013 dejó en evidencia la falta de procedimientos verificables, la poca transparencia de ciertos procesos centrales de conteo, y debilidades operativas de ciberseguridad en dichos procesos [Springall et al. 2014]. El sistema era vulnerable a la manipulación de los resultados por atacantes con recursos (otros estados) y a la instalación de malware en el software cliente. Casos similares de votación por Internet en Australia (iVote), Noruega, Suiza y Estados Unidos (Washington D.C., Utah) han mostrado dificultades similares.

En general, tanto en sistemas remotos como presenciales, el principal punto de contención es la necesidad de confiar ciegamente en que ciertos procesos (las operaciones del software cliente o del servidor, y los procedimientos de control administrativos) hayan sido realizados en forma correcta, sin que el sistema tenga mecanismos para generar evidencia sólida de tal realización. Esto genera una dependencia completamente injustificada. Si a esto le agregamos la falta de modelos claros respecto a quienes tienen acceso a votos de otros y quienes no, es posible que serias debilidades en la integridad o privacidad de estos sistemas surjan en forma indetectable.

Es difícil justificar la seguridad de sistemas de votación remota en elecciones de alto perfil y de manera sostenible en el tiempo.[4] La recomendación actual de la Academia Nacional de Ciencias, Ingeniería y Matemática (NASEM) de los Estados Unidos lo refleja bien: *"En la actualidad, Internet (o cualquier red conectada a Internet) no debiera ser utilizada para devolver papeletas de votos marcadas.[5] Más aún, la votación por Internet no debiera ser usada en el futuro hasta y a menos que garantías sólidas de seguridad y verificabilidad sean desarrolladas e instaladas, puesto que ninguna tecnología actual garantiza la seguridad, confidencialidad, y verificabilidad de las papeletas de votación marcadas si ellas son transmitidas por Internet"* [NASEM 5.11].

¿Está condenada la votación remota? No lo sabemos a ciencia cierta; solo sabemos que desconocemos cómo hacerlo bien con la tecnología actual. La única manera de saberlo con certeza es estudiándolo. La misma NASEM propone estudiarlo evaluando "científicamente los potenciales beneficios y riesgos de la votación por Internet" [NASEM 7.3].

La promesa de las nuevas tecnologías

El desafío de generar evidencia verificable de que ciertos procesos han sido llevados a cabo correctamente, puede ser alcanzado utilizando técnicas de verificación punto a punto *(End-to-end verificaction, o E2E-V)*. Usando criptografía esta técnica permite a los votantes auditar la ejecución de sistemas de votación durante la ejecución misma, en forma online. Por ejemplo, un participante externo puede matemáticamente verificar que el contenido de una encriptación es un mensaje de una forma específica, digamos la identidad de un candidato válido. Esto ha permitido diseñar sistemas donde no es necesario confiar en los participantes, basta comprobar —usando criptografía— que han cumplido correctamente su labor.

Una enorme cantidad de sistemas E2E-V han sido desarrolladas en el ámbito académico en las últimas tres décadas pero pocos han llegado a realizaciones prácticas. Entre ellas se destacan los sistemas Prêt à Voter (utilizado en Victoria, Australia [Ryan et al. 2009, Culnane et al. 2015]), Scantegrity (utilizado en Tacoma Park, Estados Unidos [Carback et al. 2010]), y STAR-vote (en Travis County, Texas, Estados Unidos [Bell et al. 2013]).

4 | Elecciones de bajo perfil, o rápidas, con sistemas nuevos y poco estudiados pueden resultar circunstancialmente exitosos (por ejemplo la consulta de municipalidades de fines de 2019). El verdadero test de efectividad está en lograr elecciones de alto perfil de manera sistemática, lo cual se conjetura infactible hoy en día.

5 | El mismo reporte efectivamente permite el envío de las papeletas originales, sin marcar, hacia los votantes, siempre que las papeletas puedan ser autentificadas (por ejemplo con una firma digital).

La seguridad de los dispositivos DRE ha sido paupérrima.

De todas maneras, las técnicas criptográficas tienen sus limitaciones: los mecanismos son usualmente complejos de entender y explicar, demandando no solo votantes activos e instruidos, sino autoridades competentes, algo no siempre posible. También requiere de implementaciones cuidadosas, pues pequeños errores de implementación en las fórmulas pueden invalidar las garantías matemáticas en las cuales se basa la seguridad del sistema (como el caso reciente del sistema de votación de la agencia postal suiza [Lewis 2019]). Aún así, NASEM recomienda tanto conducir experiencias pilotos de sistemas E2E-V que usen VVPATs [NASEM 5.10], considerando incluso su utilidad potencial una votación por Internet [NASEM 7.3].

Un concepto propuesto para votaciones electrónicas importante de mencionar es el de *independencia de software* [Rivest 2008]. Los sistemas de votación electrónicos debieran ser "independientes del software", esto es, resilientes ante fallas y errores (posiblemente maliciosos) de los computadores utilizados en dichos sistemas. Más específicamente, un sistema de votación alcanza independencia del software si un cambio o error no detectado en su software no puede causar un cambio o error no detectado en el resultado o conteo de la elección.

Una tecnología frecuentemente mencionada para votación electrónica es blockchain. Si bien la tecnología es interesante y permite resolver problemas de consistencia en sistemas distribuidos dinámicos, su aplicación a votación electrónica no es necesaria ni requerida pues los requisitos son distintos. Si bien un sistema de blockchain permitiría a una entidad publicar preferencias y registros auditables en la blockchain, su utilidad es limitada dado que la autoridad del sistema centralizado de votación siempre lo puede hacer. Además, la falta de responsabilidad de los mineros en una blockchain (algo deseable, por ejemplo, para decidir si incluir o no transacciones) resulta poco deseable en un sistema de votación donde típicamente se requiere certeza de que ciertas operaciones fueron realizadas.[6]

Otros ataques

Como indicamos al comienzo, un sistema de votación electrónica es más que el sistema para emitir y registrar las preferencias de los usuarios, e involucra, por ejemplo, los mecanismos de registro de votantes. Recientemente, debido a una posible campaña de intrusión rusa en las elecciones presidenciales de Estados Unidos de 2016, se ha puesto en discusión la debilidad de los sistemas de votación ante ataques que buscan vulnerar la integridad del registro de votantes. El objetivo de dichos ataques sería alterar, borrar personas de las listas de posibles votantes para causar confusión, molestia y apatía en el electorado, violando así el derecho al voto. Si bien la protección de dichos sistemas está muy relacionada con la discusión respecto a "segurizar la red" donde operan dichos sistemas, la existencia de requisitos legales para permitir a los ciudadanos fácilmente consultar y actualizar sus registros dificulta el proceso pues abre la puerta a ataques de ingeniería social sobre ciudadanos cuya sofisticación tecnológica puede ser baja. Asimismo, existe la posibilidad de ataques remotos ("hackeo") dirigidos no a la autoridad que ejecuta el sistema de votación sino a las empresas fabricantes de componentes del sistema. Comprometer el *software* o *firmware* de dispositivos cruciales para el conteo de votos (por ejemplo el disco duro de un sistema de conteo centralizado) pudiera ser muy efectivo a la hora de perturbar un sistema eleccionario.

Problemas abiertos

El diseño de sistemas de votación es, al fin y al cabo, la elaboración de un sistema de software confiable y usable por todos los ciudadanos de un país. Eso significa que debe proveer buena usabilidad para la mayoría de (¿todos?) los ciudadanos y generar confianza en la robustez de la implementación (esto es, la implementación no debiera tener errores).

La usabilidad de un sistema de votación es de por sí un problema complejo de múltiples aristas. ¿Podemos diseñar sistemas fácilmente usables por todos los ciudadanos, sin discriminar a un segmento de la población? ¿Cómo evitamos el *"digital divide"*, la desconexión y reticencia natural de los ciudadanos mayores ante los dispositivos tecnológicos que pudiera conspirar contra su derecho al voto? Subyacente a este problema es la disyuntiva fundamental si el ciudadano puede o debe entender el sistema de votación usado. En sistemas complejos, como los basados en técnicas criptográficas, lo más probable es que no entienda las fórmulas ni por qué los procesos funcionan. Pero ¿debe hacerlo? Un fallo de la Corte Constitucional Alemana de 2009 puso severas restricciones al uso de sistemas de votación electrónica en elecciones federales en Alemania pues "los pasos esenciales de la votación y la determinación del resultado deben poder ser examinados por un ciudadano en forma certera sin poseer conocimiento

6 | Ron Rivest recientemente dijo que implementar votación electrónica usando blockchains es como "*traer un candado a un incendio en la cocina; puede ser bueno para algunas cosas, pero no para votación*" [Rivest 2020].

especializado en el tema" [Federal Constitutional Court, 2009]. Un contraargumento es la posibilidad de todo ciudadano de viajar en aviones o consumir medicamentos sin entender su funcionamiento. ¿Hasta qué punto el carácter del sistema (elección de representantes versus transporte aéreo) debiera determinar si el ciudadano debe entender su funcionamiento por sí solo para que el sistema sea válido?

La confianza en la robustez de la solución es otro problema difícil de resolver, particularmente en una comunidad abierta y bajo el escrutinio público. ¿Cómo podemos garantizar que el software fue implementado correctamente, sin errores lógicos ni de programación? ¿Es suficiente que el proyecto sea de código abierto y sometido a auditorías periódicas? (la respuesta es negativa en ambos casos). ¿Cómo manejamos el descubrimiento y notificación de fallas de seguridad, sobre todo justo antes o durante una elección? Aún si se utilizan mecanismos de auditoría periódica, ¿cómo el votante obtiene garantías que la versión en ejecución durante la elección es la versión auditada? Y respecto al hardware, ¿debemos usar hardware genérico o especializado en los computadores utilizados? ¿Cómo garantizamos que el hardware esté libre de puertas secretas y de dispositivos de monitoreo? Estrategias existen para mitigar estos problemas pero están lejos de proveer una solución robusta y convincente para todos.

Un problema similar es crear y mantener una confianza pública en el sistema. Si bien la búsqueda continua y sistemática de fallas del sistema es un mecanismo crucial para mejorarlo, la revelación de dichas fallas pudiera aumentar la desconfianza en el mismo (la paradoja es que mientras más fallas sean encontradas y resueltas, más seguro es el sistema pero menor es la confianza de la población en el sistema). Asimismo, anuncios falsos de problemas de seguridad pueden ser difíciles de desacreditar. La principal defensa, en mi opinión, es la solidez de la confianza pública inicialmente depositada en el sistema. Ésta solo puede ser fruto de una iniciativa amplia y académicamente sólida, ojalá basada en un proceso público e iterativo con participación ciudadana transversal e inclusiva.

Desafíos de corto plazo

Mejoras parciales: un nuevo sistema de votación debiera proveer al menos los mismos beneficios y cumplir los mismos requerimientos (sino más) comparado con el sistema que reemplaza. Esto nos pone un primer desafío, el de entender el sistema actual, con sus debilidades y fortalezas. Relacionado con esto está el identificar mejoras parciales al sistema actual antes de cambiarlo por un sistema completamente electrónico (por ejemplo, la disponibilidad de un claustro electoral electrónico que permita votar en distintos locales de votación, selección más transparente de los vocales y miembros del colegio escrutador, y participación masiva en los procesos de conteo de votos). Otras mejoras incluyen fortalecer la seguridad del registro electoral online, incluyendo estrategias de detección de intentos de intrusión y alteraciones [NASEM 4.6,4.8].

Políticas públicas: desde una perspectiva más global, el Estado debiera establecer una política (estrategia) consensuada y clara que defina los procesos de estudio y cambio de sistemas electorales. Definir de manera consensuada e informada las razones y objetivos detrás de modificaciones al sistema, definiendo métricas claras de progreso [NASEM 4.10]. El establecimiento de comisiones expertas y públicas para evaluar nuevas tecnologías es también recomendado [NASEM 5.12]. Además, cualquier sistema debe ser permanentemente auditado, sus procesos y resultados, en cada elección [NASEM 5.5-5.6]. La auditoría debe ser hecha por profesionales idóneos de manera abierta y transparente, posiblemente con observadores públicos en el caso de utilizar técnicas del tipo RLA.

Investigación: el Estado debiera definir políticas claras de fomento del estudio e investigación en estos temas, incluyendo la seguridad y confiabilidad de nuevas tecnologías de autentificación de votantes, los efectos de la coerción y compra de votos (especialmente en grupos vulnerables), y evaluaciones cuantitativas respecto a si los votantes (con y sin discapacidades) podrían verificar sus papeletas de votación, y detectar errores u omisiones [NASEM 7.3].

¿Vale la pena votación electrónica?

"El propósito de un sistema de votación no es nombrar al ganador, sino convencer al perdedor". Dan Wallace, Universidad de Princeton.

La confianza en el sistema actual de votación viene de nuestra experiencia y cotidianeidad con el sistema: escribir en un papel, doblarlo, guardarlo en una caja, y luego sacarlo y abrirlo, es una experiencia relativamente común. ¿Por qué entonces quisiéramos cambiarlo? Las razones típicamente esgrimidas para introducir computadores en el proceso son muchas, desde aumentar la participación y/o facilidad de uso, hasta simplemente posibles ahorros en los costos. No es claro qué razón prima en las motivaciones, pero la experiencia comparada muestra que son la facilidad de uso, junto a la de administración y ejecución del sistema los principales factores. Sin embargo, en público frecuentemente se argumenta como beneficios de los sistemas de votación una reducción en costos, mejor usabilidad en general, y el fomento de la participación de la ciudadanía en los

procesos eleccionarios. Examinemos estas razones a continuación.[7]

Menor costo: es común argumentar que un sistema de votación electrónico (especialmente sin VVPAT) si bien pudiera tener un alto costo inicial, puede implicar un ahorro significativo en el mediano plazo, especialmente en términos de ahorros en el suministro y administración del papel. Sin embargo, tales argumentos son debatibles pues no consideran los nuevos costos: el almacenamiento seguro, entrenamiento del personal, licenciamiento de software, y la reparación y actualización de los equipos y dispositivos [Zetter 2008].

Mejor usabilidad: aparte de dificultades asociadas al *"digital divide"*, el diseño de la interfaz de un sistema de votación electrónica requiere estudios cuidadosos de la población objetivo, lo cual no siempre es fácil ni da los resultados deseados [Herrnson et al. 2006; Oostveenet et al. 2009]. Además, puede introducir nuevos problemas de usabilidad [Conrad et al. 2009], posiblemente aumentando las tasas de voto fallido *(undervote)* [Acemyan et al. 2014]. No es sorprendente por lo tanto la recomendación de la NASEM respecto a utilizar asesoría especializada para diseñar tanto la interfaz (audio y pantalla) como la impresión de las papeletas de nuevos sistemas de votación electrónico con apoyo [NASEM 4.9].

Aumento de la participación: un argumento frecuentemente mencionado es que los votantes participarían más en votaciones remotas por la facilidad de no tener que desplazarse físicamente. Diversos estudios cuestionan esta conclusión. El estudio de Bochsler aplicado al caso Estonia en 2007 argumenta que "en vez de atraer nuevos votantes, pareciera que la votación por Internet principalmente sustituye a los votantes en las urnas" [Bochsler 2010]. Otro, de 2017 sobre dos circunscripciones en Holanda, reportó "ningún efecto en la participación" [Germann et al. 2017]. Y un estudio en Canadá sí detectó un aumento de participación de un 3.5% e incluso mayor en situaciones donde no existe voto por correo o el registro previo no es obligatorio pero comparable con aumentos obtenidos vía flexibilizaciones similares de las reglas para participar en la votación. El mismo estudio sin embargo concluye que, "si bien la votación por Internet puede mejorar la participación, es improbable que resuelva la crisis de participación". En resumen, la evidencia científica justificando un incremento en la participación sería aparentemente escasa.

Otras razones: pese a las (aparentemente) malas noticias anteriores, existen otras razones raramente mencionadas pero sin embargo beneficiosas de la votación electrónica. Estos sistemas tienen la potencialidad de permitir mejorar la usabilidad e inclusión para comunidades típicamente ignoradas, como ciudadanos con discapacidades (por ejemplo, interfaz de audio para personas con dificultad visual, distintos colores para gente con dificultad visual, o incluso pedales para personas con discapacidades en su torso superior), ciudadanos cuyo lenguaje no es el mayoritario en un país (por ejemplo, personas de habla Quechua o Mapudungún), o permitir mayor flexibilidad en el tipo de preguntas, permitiendo preguntas potencialmente más complejas (varias opciones rankeadas, por ejemplo). Lamentablemente, estos beneficios por sí solos no parecen ser suficientes cuando el sistema no cumple los requerimientos fundamentales enunciados al comienzo de este artículo.

Quizás el aspecto más interesante y prometedor es la posibilidad futura de construir variantes de sistemas de votación electrónica que permitan una interacción continua y fluida entre la ciudadanía con sus representantes, así como entre los distintos ciudadanos. Canalizar la voz de los ciudadanos en forma eficiente en procesos de participación democráticos preservando la seguridad es el gran desafío de los próximos años.

Conclusión

Los sistemas de votación son una pieza clave en nuestros procesos democráticos y su modificación no debe tomarse a la ligera. La introducción de sistemas electrónicos de votación, si bien presenta algunos beneficios, actualmente conlleva riesgos demasiado significativos comparados con la operación del sistema actual. Mientras la tecnología existente no permita minimizar y acotar dichos riesgos, no es claro que tal migración sea recomendable. Obviamente, eso no significa dejar de estudiar o testear nuevas técnicas y prototipos de votación. Todo lo contrario: nuestra sociedad, en conjunto con académicos, investigadores e innovadores, debiera hacer un esfuerzo por analizar los actuales desafíos, diseñar nuevos sistemas y experimentar con su aplicación específica a nuestra comunidad. El conteo local de votos, la generación de trazas en papel (VVPAT) con protección legal adecuada, el uso de técnicas criptográficas E2E-V para lograr independencia del software, y las auditorías estadísticas (RLA) post elección, son herramientas que debieran ayudarnos. Sin embargo, faltarán nuevos mecanismos y nueva ciencia, cuya creación no será trivial. Mejorar la calidad de la democracia, con mejor y mayor participación ciudadana nunca ha sido fácil. Pero ciertamente siempre ha valido la pena hacerlo. ▪

7 | Esta sección está basada en [Hevia 2018].

REFERENCIAS

- [Acemyan et al. 2014], "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II.". C. Z. Acemyan, P. Kortum, Michael D. Byrne y D. S. Wallach. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections, 2014.
- [Arahna et al. 2019], "The Return of Software Vulnerabilities in the Brazilian Voting Machine", D. F. Aranha, P. Y. S. Barbosa, T. N. C. Cardoso, C. Lüders de Araújo y P. Matias. Elsevier Computers & Security, 86, 2019.
- [Bell et al. 2013], "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System", S. Bell, J. Benaloh, M.D. Byrne, D. Debeauvoir, B. Eakin, G. Fisher, P. Kortum, N. McBurnett, J. Montoya, M. Parker y O. Pereira. USENIX Journal of Election Technology and Systems, 1(1), 2013.
- [Bochsler 2010], "Can Internet voting increase political participation", D. Bochsler. En conferencia 'Internet and Voting', Fiesole, 2010.
- [Carback et al. 2010], "Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy". R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen y A. T. Sherman. USENIX Symposium, 2010.
- [Conrad et al. 2009], "Electronic voting eliminates hanging chads but introduces new usability challenges", F. G. Conrad, B. B. Bederson, B. Lewis, E. Peytcheva, M. W. Traugott, M. J. Hanmer, P. S. Herrnson, R. G. Niemi. Int. J. Human-Computer Studies 67, 2009.
- [Culnane et al. 2015], "vVote: a verifiable voting system". C. Culnane, P. Y. Ryan, S. Schneider y V. Teague. ACM Transactions on Information and System Security, 18(1), 2015.
- [Feldman et al. 2006], "Security Analysis of the Diebold AccuVote-TS Voting Machine", A. J. Feldman, J. A. Halderman y E. W. Felten, 2006. https://citp.princeton.edu/our-work/voting/
- [Germann et al. 2017], "Internet voting and turnout: Evidence from Switzerland". M. Germann y U. Serdült. Electoral Studies, 47, Elsevier, 2017.
- [Gonggrijp et al. 2007], "Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective", R. Gonggrijp y W-J. Hengeveld. USENIX workshop on accurate electronic voting technology, 2007. http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf
- [Herrnson et al. 2006], "The Importance of Usability Testing of Voting Systems", P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, M. Traugott. USENIX/ACCURATE Electronic Voting Technology Workshop. 2006.
- [Hevia 2018], "El Camino hacia la Votación Electrónica Segura en Chile", presentación en Conversatorio "Ciberseguridad, ¿estamos preparados?", A. Hevia. Senado de Chile, 6 de Julio de 2018.
- [Kiayas et al. 2006], "Security Assessment of the Diebold Optical Scan Voting Terminal", A. Kiayias, L. Michel, A. Russell, A. A. Shvartsman, M. Korman, A. See, N. Shashidhar y D. Walluck. (2006). https://web.archive.org/web/20061127175659/http://voter.engr.uconn.edu/voter/Reports_files/uconn-report-os.pdf
- [Lewis 2019], "Ceci n'est pas une preuve: The use of trapdoor commitments in BayerGroth proofs and the implications for the verifiability of the Scytl Swiss Post Internet voting system", S. J. Lewis, O. Pereira y V. Teague. Univ. Melbourne, Australia, 2019.
- [NASEM], "Securing the vote", National Academy of Sciences, Engineering, and Math, 2018.
- [Oostveenet et al. 2009], "Users' experiences with e-voting: A comparative case study", A. M. Oostveen y P. den Besselaar. Journal of Electronic Governance 2, no. 4, 2009.
- [Rivest 2008], "On the notion of 'software independence' in voting systems", R. L. Rivest. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 366, no. 1881, 2008.
- [Rivest 2020], "Cryptographers Panel" en RSA Security Conference, febrero de 2020.
- [Ryan et al. 2009], "Prêt à voter: a voter-verifiable voting system". P. Y. Ryan, D. Bismark, J. Heather, S. Schneider y Z. Xia. IEEE transactions on information forensics and security, 4(4), 2009.
- [Springall et al. 2014], "Security Analysis of the Estonian Voting System", D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine y J. Alex Halderman. CCS 2014 "Independent Report on E-voting in Estonia", https://estoniaevoting.org/ 2014.
- [Wolchok et al. 2010], "Security Analysis of India's Electronic Voting Machines", S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati y R. Gonggrijp. En ACM Conference on Computer and Communications Security, 2010.
- [Wolchok et al. 2012], "Attacking the Washington, DC Internet voting system", S. Wolchok, E. Wustrow, D. Isabel y J. A. Halderman. International Conference on Financial Cryptography and Data Security, Springer, 2012.
- [Zetter 2008], "The Cost of E-Voting", K. Zetter (4 de abril de 2008). https://www.wired.com/2008/04/the-cost-of-e-v/