VOTACIÓN ELECTRÓNICA: AVANCES, DESAFÍOS Y OBSTÁCULOS

EN NUESTRO PAÍS DESPUÉS DE CADA ELECCIÓN SE INSTAURA EL TEMA DE LA VOTACIÓN ELECTRÓNICA PARA FACILITAR Y MEJORAR EL ACCESO A LOS VOTANTES, Y ES JUSTO EN ESE MOMENTO, DONDE SE MENCIONA LA IDEA DE "VOTAR DESDE LA CASA". SI BIEN LA IDEA ES BRILLANTE, PARA LOGRARLO AÚN QUEDAN MUCHOS DESAFÍOS POR DELANTE.

MARIOCORNEJO

Magíster (c) en Ciencias mención Computación, Departamento de Ciencias de la Computación Universidad de Chile. Co-fundador de E-Voting Chile, empresa dedicada a la investigación aplicada, implementación y divulgación en temas de votación electrónica.

mcornejo@dcc.uchile.cl

UN PROCESO COMPLEJO

En general el proceso eleccionario es uno de los más importantes de las democracias modernas, incluso en las actuales monarquías se utiliza para escoger al Primer Ministro, parlamentarios, alcaldes, etc. Este proceso es complejo y más aún cuando cada nación tiene su propio sistema electoral, donde unos eligen a sus representantes a través de voto universal (todos los votos cuentan) y otros a través de voto indirecto, donde se vota a un delegado quién representa una cierta cantidad del electorado. Adicionalmente la forma de elegir a los ganadores también es distinta en cada país, algunos tienen sistemas directos, proporcionales, semiproporcionales y cómo no mencionar nuestro sistema binominal.

Los sistemas electorales basados en papel como el chileno (y en particular como el chileno, donde el voto se emite en papel en una cámara secreta para ser depositado luego en una urna cerrada), derivan distintas propiedades desde el mundo real que nos parecen muy naturales. Entre ellas podemos mencionar:

PRIVACIDAD

Se obtiene al marcar una opción en la cámara secreta y al depositar la papeleta en una urna cerrada.

EQUIDAD

Las cámaras secretas de votación aseguran que los votantes no pueden ser influenciados y las urnas cerradas previenen resultados tempranos.

VERIFICACIÓN Y CORRECTITUD

Transparencia del proceso y la imposibilidad de cambiar un voto ya depositado en la urna.

Junto a estas propiedades y la existencia de una cultura del "deber cívico", expresada en el acto de participar como vocal de mesa y/o sufragando, permite construir sociedades en donde sus integrantes se sientan parte de su construcción.

E-VOTING

Michael Remmert en [1] da una definición sobre votación electrónica (*e-voting)* como una votación o referéndum que involucra el uso de dispositivos electrónicos, al menos para marcar una preferencia. Según esta definición, la utilización de voto electrónico no es nueva en el mundo: en 1964 en los condados de Fulton y DeKalb en Georgia, se utilizó por primera vez un sistema donde se perforaban tarjetas, las cuales facilitaban el conteo automatizado. Afortunadamente, cuando hoy hablamos de e-voting, automáticamente pensamos en dispositivos *"touchscreen"* y en ningún caso en la utilización de tarjetas perforadas.

→

Si bien, cada sistema es singular, existen algunas características deseables transversales a todos los sistemas de votación como el **anonimato del voto**, el cual nos garantiza que nadie puede conocer el voto de otra persona (más allá de lo posible de deducir a partir del total), el voto debe ser el deseo del votante y **sin presión de ningún tipo** (coerción). Además, se espera que el sistema **no permita la venta de votos** (cohecho), que tenga alguna medida de **anticolusión** al momento de contar los votos (por ejemplo vocales de mesa escogidos al azar) y por supuesto que la **suma de estos sea correcta** (apoderados de mesa verificando cada uno de los pasos).

La idea principal de la votación electrónica moderna es alcanzar estas propiedades usando técnicas computacionales, y para esto se utilizan herramientas matemáticas criptográficas. Dichas herramientas permiten crear sistemas de votación electrónica capaces de garantizar las propiedades antes mencionadas. Más aún, permiten verificar matemáticamente y de forma online que dichas propiedades se alcancen, algo que las votaciones en papel no permiten. Una de estos sistemas es el basado en un tipo especial de encriptación, denominado encriptación homomórfica, como el esquema de encriptación de Paillier [2], el cual permite el anonimato del voto. Este esquema es homomórfico con respecto a la suma, esto quiere decir, que no es necesario abrir cada uno de los votos para sumarlos, ya que tan sólo con multiplicar los valores encriptados se obtiene el resultado de la votación. Usando esta técnica en ningún momento se abren los votos individuales y, por tanto, se mantiene el anonimato en todo momento.

Para desencriptar la suma de los votos se necesita una llave privada, lo que introduce el problema que una única entidad (o persona) puede arbitrariamente concentrar todo el poder. Sin embargo, es posible "repartir" esta llave secreta utilizando una técnica llamada ***secret sharing*** [3]: la llave se divide en ***n*** pedazos, y se fija un umbral de al menos ***k*** para poder desencriptar la suma de los votos.

Adicionalmente, las herramientas criptográficas nos permiten hacer algo casi mágico: adjuntar una especie de *hash* o *checksum* como una garantía de "buen comportamiento" al momento de votar. Esto se realiza mediante la utilización de una ***zero knowledge proof*** [4], la cual nos asegura que todos los cálculos fueron correctamente hechos sin revelar ninguna información privada sobre el cálculo. Con ésta técnica es posible asegurar que la suma total de votos es correcta y consistente con todos los votos emitidos.

Utilizando estas propiedades es posible asegurar que el administrador de sistema o el administrador de la base de datos (en realidad, cualquiera que tenga acceso al servidor) no pueda conocer el contenido de los votos y tampoco adulterarlos. En la actualidad algunos municipios y organizaciones sociales utilizan el nombre de "votación electrónica", cuando en realidad lo que hacen es simplemente una *encuesta de opinión*, sin ningún tipo de protección contra fraude o anonimato del voto.

En general, existen dos formas de votar electrónicamente, una llamada **presencial**, en la cual el votante se apersona en un centro de votación, y otra llamada **remota,** en la cual se vota desde cualquier parte, en particular desde la casa o del lugar trabajo.

VOTACIÓN ELECTRÓNICA PRESENCIAL

Entre las múltiples ventajas comparativas al momento de hablar de votación electrónica presencial, quizás la más fuerte, es que mantiene el nivel de confianza que tiene la votación basada en papel en los aspectos relacionados con verificación de la identidad del votante, en particular, que éste se encuentre habilitado para votar; la privacidad del voto, y que el votante lo haga sin presiones ni influencias.

La lógica de la votación tradicional se mantiene, donde un votante acude a un centro de votación y los vocales de mesa verifican su identidad. Luego el votante entra a la cámara secreta y marca una preferencia en un computador (o similar), en vez de hacerlo en una papeleta. Una vez finalizada la elección, los votos son contados en cada centro de votación o de forma centralizada según sea el caso.

VOTACIÓN ELECTRÓNICA REMOTA

La votación electrónica remota, a diferencia de la presencial, nos permite sufragar desde cualquier parte, como por ejemplo desde la casa. En términos prácticos, uno se conecta a una página web, inicia sesión y luego vota. Al votar remotamente se relajan algunas propiedades, como la verificación de la identidad del votante, ya que ningún mecanismo biométrico sin supervisión es 100% confiable. Tampoco es posible saber si el votante lo hace libremente y sin presiones, o si está recibiendo dinero por emitir el voto.

La votación remota tampoco es algo nuevo, en países como Estados Unidos, España, Reino Unido, Italia, entre otros, es posible votar a través de correo postal o fax. Incluso en Francia es posible autorizar a otra persona para votar en caso de no poder concurrir al centro de votación.

El voto postal sugiere otra relajación a los sistemas de votación, ya que eventualmente el voto podría perderse, ser abierto, nunca ser sumado, etc. Sin embargo, se utiliza en países con historia democrática y al parecer a los ciudadanos de esos países no parece importarle. La diferencia con los sistemas de votación electrónica remo-

ta es que es posible montar un ataque a gran escala sin tantos recursos y de forma silenciosa. Montar un ataque a un sistema de votación remota postal, requiere mucho esfuerzo, tiempo, dinero y una logística que no es fácil de lograr (requiere conocer a quienes votan por correo postal, enviarles un carta con un voto suplantando al registro electoral, etc.)

¿PODEMOS APLICARLO EN CHILE?

¡Por cierto que sí!

La votación electrónica parece ser la modernización de la actual forma de votar, mejorando el acceso a votar desde cualquier centro de votación (ya que el padrón se encuentra *online*). En particular, permitiría votar desde el extranjero y evitaría tristes episodios, como los vividos en la elección municipal de 2012, cuando se perdieron votos. Además, posiblemente aumentaría la velocidad en el conteo de votos y la comodidad de los votantes.

Por otro lado, no tan sólo se podría usar como herramienta de elección de autoridades, sino también como herramienta en la toma de decisiones comunales, regionales e incluso legislativas.

Desde un punto de vista tecnológico, existe el conocimiento y las personas capacitadas para poner en marcha un proyecto así. También existen los algoritmos y protocolos hace ya varios años. Los obstáculos, a mi parecer, radican en la brecha digital, el desconocimiento (por parte de las autoridades y de los ciudadanos) y la voluntad política para implementarlo. ■

REFERENCIAS

[1] Remmert Michael. "Towards European Standards on Electronic Voting". Electronic Voting in Europe 2004. pp. 13-16.

[2] Paillier, Pascal. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". EUROCRYPT 1999.Springer. pp. 223–238.

[3] Shamir, Adi. "How to share a secret". Magazine Communications of the ACM, Volume 22 Issue 11, Nov. 1979, pp 612-613.

[4] Goldwasser, S.; Micali, S.; Rackoff, C. "The knowledge complexity of interactive proof systems", SIAM Journal on Computing 1989. pp. 186–208.