

## “Un Estado democrático debería garantizar el voto secreto” » Noticias Urbanas

Por Florencia Galarza / 13 de septiembre 2016

A un año de las elecciones legislativas, y a tres meses de que pueda legalizarse el voto electrónico en todo el país, Noticias Urbanas consultó a expertos informáticos para conocer más sobre la BUE.



El proyecto de ley se encuentra en tratativas.

A fin de conocer por qué la implementación del voto electrónico significa una amenaza a la soberanía y derechos constitucionales de los argentinos, *Noticias Urbanas* consultó a **Javier Smaldone**, consultor de software y administrador de sistemas, especialista en este rubro.

A sólo tres meses para que el proyecto de ley denominado “**Reforma política**” sea sancionado, o al menos así lo espera el Ministerio de Gobierno porteño, impulsor de dicho proyecto, **el 75**

**por ciento de la Ciudad mantiene un visto bueno sobre Vot.ar,**  
este sistema electoral.

La digitalización del sufragio promete convertir al proceso  
eleccionario en “fácil, rápido y moderno”, eliminar las “boletas  
sábanas” y, por ende, aportar transparencia. Pero, en realidad,  
**Vot.ar pondría en jaque el artículo 37 de la Constitución: el  
derecho al voto secreto, universal, igual y obligatorio, rasgo  
esencial de un Estado democrático.**

Con esto, **Juan Manuel Urtubey** argumenta que este sistema evita  
el robo de boletas, por lo que ya no sería necesaria la fiscalización,  
ni el control del escrutinio, así como tampoco la reposición de las  
boletas, ya que **el proceso eleccionario sería más rápido y  
prolijo y de “una seguridad absoluta”.**

Votar a través de computadoras, mecanizar el conteo, mantener  
sistemas de registros electrónicos sería exponer a la voluntad del  
votante a la voluntad de máquinas encriptadas cuyos controles son  
remotos. Sistemas que, según profesionales de la informática, son  
de “muy fácil hackeo”.

### **Mitos del voto electrónico**

Aunque uno de los argumentos oficiales para implementar este  
sistema de votación es “su utilización por parte de los países del  
primer mundo”, **el voto electrónico es utilizado sólo por tres  
países: India, Venezuela y Brasil;** mientras que Bélgica y Estados  
Unidos lo utilizan de manera parcial.

Así, **“los países del primer mundo” fueron descartándolo  
progresivamente por detectar sabotajes y todo tipo de  
irregularidades.**

“La objeción más fuerte al uso de computadoras para votar es que  
el votante debe enfrentarse a un sistema informático para expresar

su voluntad, el cual no puede controlar, no puede saber cómo funciona, o si es seguro”, indicó Javier Smaldone. Y completó: “Al no constarle al votante que se respeta su derecho del voto secreto, si éste estuviese en una situación de vulnerabilidad y es cohesionado por un puntero político, **tras la amenaza de que podrá saber a quién votó, basta para que agache la cabeza y vote como le piden o pagan**”.

De esta manera, **flaquearía el segundo argumento oficial: “la disolución del clientelismo eleccionario”**, el cual “no desaparece, sólo se les da nuevas herramientas”.

Por su parte, **Beatriz Busaniche**, presidente de la fundación Vía Libre, desterró un tercer mito en el marco de un foro sobre el voto electrónico realizado el pasado martes 6 en el teatro Ateneo: **“Nos venden que con el voto electrónico terminaría la lista sábana. Pero esto es una gran mentira, sólo la esconde.** En el texto de la reforma indica que en la pantalla de votación se debe mostrar entre uno y tres de los candidatos legislativos. El resto de la lista no va a estar disponible en la pantalla. Uno va a votar a ciegas”. Así, Venezuela es el ejemplo más cercano de la posibilidad de la filtración de datos de los votantes:

### **Una impresora no tan “boba”**



El mismo **Sergio Angelini**, presidente de **Magic Software Argentina (MSA)** que es proveedora de este sistema, insistió en que la “impresora” de las boletas es una “máquina boba” a fin de demostrar la transparencia de su tecnología.

En tanto, Smaldone refutó: “Es una impresora que tiene cuatro puertos USB, lector de audio, memoria, sistema operativo y

un pequeño sistema oculto. Se trata de un cable que da acceso de todo el control sobre la máquina y está presente durante las elecciones. Este cable tiene la capacidad de almacenar, por ejemplo, qué se votó y en qué orden. No sabemos si lo hace, pero tiene toda la capacidad para hacerlo”.

### **El riesgo de las auditorías**

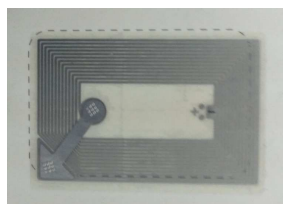
Si hay algo que evidencia la falta de transparencia de este sistema es “la necesidad de auditorías”. “En este punto, cabe destacar que por más seria y bien hecha que sea una auditoría, nunca hay garantías 100 por ciento de una el sistema no tenga algún problema”.

El ejemplo más concreto radica en las auditorías que se realizaron en las últimas elecciones para jefe de Gobierno porteño y para gobernador en Salta. “Ese sistema fue auditado, en particular, por el equipo de una Universidad Nacional de Salta y por el de la Universidad Nacional de Bs. As. **Y aunque fueran oficiales y encargadas por la justicia electoral, no encontraron problemas graves que sí fueron detectados por investigadores independientes, que lo hicieron con recursos mínimos**”, señaló el experto informático.

[Así, viene a cuento el caso de Joaquín Sorianello, el informático que había podido acceder a datos confidenciales de este sistema desde su computadora domiciliaria.](#)

### **Boletas con chips: una ventana abierta**

Las boletas electrónicas tienen incorporado un pequeño **chip**



**RFID**, encargado de almacenar la información del voto. Mientras que la máquina de votación contiene una

pantalla para presionar al candidato elegido y una entrada para la lectura y grabado de la boleta. Ésta es la misma que se usa para votar, contar los sufragios y hacer escrutinios.

En tanto, el presidente de mesa cuenta con una credencial con otro chip con sus datos, y son portadores de actas de inicio, cierre y escrutinio que también almacenan información en chips. Este último es el encargado de iniciar la máquina con un DVD luego de identificarse.




Hasta este punto del proceso electoral, Smaldone realizó varias observaciones: “Cada identificación y acta tienen chips con números iguales (y no están cifrados), sólo cambia un número de registro. **Entonces, cualquiera con un celular u otro dispositivo podría realizar esas grabaciones y fabricar actas de apertura o identificaciones. No se necesita nada más**”.

De la misma manera, una vez seleccionada en la pantalla el candidato a votar, el votante debe verificar que lo que marcó es lo que se grabó en el chip, es decir, **“le estamos pidiendo a la misma máquina que nos muestre lo que contiene la boleta”**.

Smaldone también indicó que existen sistemas remotos diseñados para “leer, quemar o sabotear” a la distancia indicada el contenido de los chips, desde el mismo celular u otros dispositivos: “Si uno va a las especificaciones del fabricante de estos chips dice que tienen una lectura posible desde unos 50 cm de distancia”.

**“Está comprobado que pueden leerse los votos con un celular y hacer una app que permita la compra de votos, almacenar varios votos en una misma boleta, y que después se contarán varios votos en uno”**, resumió Smaldone.

Luego, en el escrutinio provisorio se toma una computadora de la escuela que debe conectarse a Internet de alguna forma, y así se conecta con el centro de cómputos y se transmiten cada una de las actas. Sin embargo, en las últimas elecciones “hubo sistemas que fallaron” y debieron enviarlas “en taxis”.

<b>MEMORIA DESCRIPTIVA DE LA PATENTE DE INVENCIÓN</b>		Otro objeto del presente invento es proveer medios para determinar que toda boleta que los electores depositen en la urnas contenga un voto, aún cuando este voto sea un voto en blanco.
<b>SOBRE:</b>		Otro objeto del presente invento es proveer de medios para asegurar el secreto del voto en la boleta de voto electrónico, entre los que se encuentra la lectura de la totalidad de los TAG-RFID dentro de la Urna, sin necesidad de tener que abrirla, evitando todo contacto manual con los votos.
<b>DISPOSICIÓN Y MÉTODO DE VOTO ELECTRÓNICO</b>		Aún otro objeto del presente invento es un método de utilizar la disposición de voto electrónico para ejercer el acto de votación.
<b>SOLICITADA POR:</b> MSA Magic Software Argentina SA		Un objeto adicional del presente invento es asegurar mediante el método de votación empleado, una natural aleatoriedad de grabado de votos en la respectiva base de datos, imposibilitando toda correlación entre datos registrados secuencialmente y origen de dichos datos con las listas de los
<b>CON DOMICILIO EN:</b> Av. Corrientes 640 Piso 10 Of. 1 y 2 C1043AAT Buenos Aires Argentina		
<b>POR EL PLAZO DE VEINTE AÑOS</b>		

## De puño y letra

Los mismos impulsores y defensores de este sistema cometen errores tanto en sus procesos de votación y traspiés en sus discursos que exponen las vulnerabilidades de Vot.ar. La secretaria del Tribunal Electoral de la Provincia de Salta, **Teresa Ovejero**, fue quien aseveró: **“Si el CD que lleva la máquina, que es el que tiene el sistema operativo, si de repente cayera en manos de una persona inescrupulosa que quisiera hacerle un daño al sistema, puede cambiarlo a ese software y puede ahí sí tratar de meter un CD en una máquina, en connivencia con una autoridad de mesa o con alguien, y ahí sí uno va a apretar para votar a tal y va a salir a cual”.**

De esta manera, se comprende que si toda la seguridad del sistema de votación depende de algo tan sencillo como que alguien no cambie el CD, Vot.ar mantiene una vulnerabilidad extrema que no requeriría mayor argumentación.

## La Ciudad: la prueba piloto



Durante las elecciones del 5 de julio del pasado año en la Ciudad no sólo falló la transmisión de los datos y las últimas urnas con las actas debieron ser llevadas a las centrales de cómputos en taxis, sino que el resultado también sufrió imperfecciones.



A las 21.57 había un 92,5 por ciento de mesas escrutadas; mientras que a las 2 había un 95 por ciento, es decir, sólo un 2 por ciento fue escrutado en 4 horas. Mas el otro 5 por ciento no se escrutó nunca.

Otro dato fallido. A las 21.57 había 147.100 electores en total, y 147.363 votos emitidos. Había mas votos que votantes, que encima “representan el 71,8 por ciento”.