El elemento de votación y el secreto del voto

Javier Smaldone

Por estos días en la Argentina se está discutiendo la reforma del sistema electoral. En particular, la del sistema de votación. Casualmente, acaban de cumplirse cien años de la primera elección realizada bajo la llamada Ley Sáenz Peña. Sin embargo, en persecución de una supuesta modernidad, muchos parecen olvidarse del aporte fundamental de esta ley al sistema democrático argentino: la garantía del secreto del voto.

Así se oponía el estanciero, ex ministro del autonomismo y profesor de Derecho Constitucional de la UBA, Carlos Rodríguez Larreta al punto más importante del proyecto de Sáenz Peña:

> Si mi peón hubiera tenido la misma acción que yo para resolver los problemas económicos internacionales, o políticos del país, habríamos estado viviendo bajo un régimen absurdo. No ha sido así, gracias a Dios, porque yo he dirigido a mi peón. Pero el voto secreto lo independiza, al privarlo de una influencia

saludable y legítima... Y lo malo es que a menudo no tenemos un solo peón sino varios, y que algunos tienen muchos.[1]

Y, dados los intereses que defendía, razón no le faltaba.

Por otro lado, de esta forma relató las consecuencias de la primera votación en un cuarto oscuro, con voto secreto, el historiador Félix Luna:

> Así llega el 7 de abril. Se vota con tranquilidad en todo el país. En la Capital Federal la Unión Nacional compra votos descaradamente. No pocas incidencias ocurren con este motivo. Los comités de la Unión Nacional están atestados de ciudadanos. En uno de ellos don Tomás de Anchorena pregunta uno por uno a los votantes:
> –¿Votaste bien, m'hijito...?
> –Sí, doctor –era la respuesta obligada.
> –Bueno, tomá diez pesos...
> En esas condiciones resultó inexplicable para muchos el resultado de la Capital: triunfo radical, minoría socialista... La oligarquía, los círculos oficiales no comprendían que el pueblo porteño, con su escondida picardía, se había dado el gusto de "burlar a los eternos burladores y al mismo tiempo, votar a la novia del corazón: Hipólito Yrigoyen...", como dice agudamente un escritor antiyrigoyenista.[2]

Tiempo después, en el Congreso, el presidente Roque Sáenz Peña resumiría magistralmente en una frase los efectos que causó la instauración del secreto del voto:

> Si hubo votos pagados, no hubo votos vendidos.[3]

---

1 Sampay, Arturo, *Constitución y pueblo*, Buenos Aires, Cuenca ediciones, 1974.

2 Luna, Félix, *Yrigoyen*, Buenos Aires, Sudamericana, 1999.

3 *Ibíd.*

Estancieros modernos

Desde las elecciones provinciales y nacionales de 2015, se han difundido numerosos informes periodísticos sobre el accionar de la versión moderna de don Tomás de Anchorena y sus esbirros: flotas de automóviles de alquiler –incluso motocicletas– usados como transporte de votantes, quienes reciben bolsones de alimentos, dinero en efectivo y hasta viviendas a cambio de "votar bien". El llamado "clientelismo político" sigue estando, un siglo después, a la orden del día.

Pero, ¿por qué funciona? Porque cuando el sistema de votación era novedoso desconcertó a quienes querían cometer fraude, pero con el paso del tiempo estos fueron "tomándole la mano". Lo mismo ocurre con cualquier sistema: cuando es puesto en funcionamiento, salvo fallas evidentes, todo marcha bien. Pero luego van apareciendo formas de explotar sus vulnerabilidades o de trampearlo. Y al sistema actual de votación se le han encontrado varias.

"Tomá esta boleta. Es la que tenés que poner en el sobre. Tiene una marquita aquí, ¿la ves?". "Nuestro fiscal va a firmar tu sobre de forma en que podamos saber a quién votaste. Más te vale que cumplas con el trato". Frases como estas son pronunciadas por los "punteros políticos" –delegados de la versión moderna de aquel estanciero– a los votantes al entregar el dinero en efectivo, el bolsón, o el plan social.

¿Podrá el fiscal identificar la boleta con la supuesta marca entre más de 200 que habrá en la urna? ¿Será cierto que tiene una forma de "firma codificada" para saber a qué votante pertenece cada sobre? Posiblemente no, pero... ¿estará dispuesto quien recibió un pago por su voto a correr el riesgo de traicionar al puntero? ¿O el voto comprado se transformará, ante la duda y el temor, en voto vendido? Dados los ingentes recursos que se destinan a estas maniobras, todo parece indicar que esto último es lo que en efecto sucede. La coerción resulta efectiva.

La garantía del secreto

Para que el secreto del voto ocasione el efecto deseado –nada menos que la libertad de elegir– es el votante quien debe estar seguro de su garantía. Y el sistema debe permitírselo. Si quien es presionado no puede asegurarse por sus propios medios de que nadie puede saber cómo votó, la presión surtirá efecto. En esto, el sistema electoral es como la esposa de Julio César: "Además de ser honesta, debe parecerlo".

La reforma electoral impulsada desde el gobierno actual –y que cuenta con el apoyo mayoritario de fuerzas políticas y el público en general– introduce un nuevo elemento entre el votante y la expresión de su voluntad: un sistema informático. El procedimiento de emisión del voto parece bastante robusto desde el punto de vista de asegurar que el escrutinio reflejará la selección realizada por el ciudadano frente a la computadora. La máquina permite seleccionar los candidatos en la pantalla, y luego imprime voto en una boleta de papel, y lo almacena en un chip de identificación por radiofrecuencia (RFID) contenido en la misma. El votante tiene la posibilidad de leer lo impreso, y hasta de ver lo que está grabado –en realidad, lo que la máquina le dice que está grabado– en el circuito electrónico embutido en el papel. Luego, en el escrutinio, los votos deberán contarse para poder verificar que lo impreso coincida con lo almacenado digitalmente. Ante la discrepancia o la duda deberá prevalecer lo escrito en el papel (en una instancia posterior, ya que el resultado de la mesa se basará no en lo que sus integrantes puedan leer, sino en lo que la computadora pueda contar).

Más allá de las particularidades técnicas de este sistema propuesto llamado "boleta única electrónica" –del cual existe solo una implementación en el mundo, perteneciente a una empresa privada–, ¿cómo puede el votante estar seguro de que su voto es secreto, cuando debe emitirlo mediante una computadora? La respuesta corta es: *no puede*.

Y aquí de nada sirven las auditorías (menuda tarea, si acaso posible, para un sistema de tal complejidad). El solo hecho de

que el medio de votación requiera de auditorías especializadas demuestra que el mismo no puede ser controlado por el votante, y esto debería disparar todas las alarmas. No se trata de si un grupo de personas con los conocimientos técnicos y los recursos apropiados puede –dado un tiempo razonable– asegurarse de que el sistema garantiza el secreto. Se trata de que el votante, parado frente a una computadora, pueda estar seguro de que la amenaza del puntero –"votá bien, porque tenemos las computadoras tocadas y vamos a saber a quién votaste"– no tiene asidero. Lamentablemente, esa seguridad del votante no es posible.

¿Cómo puede violarse el secreto mediante una computadora de votación? Las formas son variadas y sorprendentes. Desde la decodificación de emisiones electromagnéticas[4] (técnica conocida como *interferencia de Van Eck*),[5] hasta la utilización de componentes no previstos ni auditados[6] que permitan almacenar el orden y la composición de cada voto. Y en el caso de usar chips como el de la "boleta única electrónica", existe incluso la posibilidad de leer el contenido de la boleta desde cierta distancia.[7] Ni qué decir de las nuevas formas en que se puede obligar a un votante a demostrar si "votó bien", algunas tan simples como la utilización de un celular oculto.[8]

Puede argüirse –en un ejercicio de ingenuidad– que estas prácticas son demasiado complejas o rebuscadas. Ante cada posibilidad de vulnerar el secreto puede ofrecerse una solución a modo de paliativo. Pero el hecho es que el ciudadano común (y aun el experto en informática) no podrá,

---

4 Este video ilustra cómo funciona dicha decodificación: https://www.youtube.com/watch?v=hwz1BLRgTgo

5 Más información sobre esta técnica en https://es.wikipedia.org/wiki/Interferencia_de_Van_Eck

6 "El sistema oculto en las máquinas Vot.ar", 15/07/2015, https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar/

7 "Sobre el chip RFID de la 'boleta única electrónica'", 08/01/2016, https://blog.smaldone.com.ar/2016/01/08/sobre-el-chip-rfid-de-la-boleta-unica-electronica/

8 "Comprando votos con la boleta única electrónica", 03/09/2015, https://blog.smaldone.com.ar/2015/09/03/comprando-votos-con-la-boleta-unica-electronica/

parado frente a una computadora en el momento de elegir a sus representantes, saber a ciencia cierta que nadie lo está espiando a través de ese sistema.

Fácil y rápido, como antes de 1912

Antes de la Ley Sáenz Peña, votar era muy simple. No había discusiones sobre boletas, sobres, ni máquinas de ningún tipo. Los ciudadanos desfilaban ante la mesa, expresaban su voluntad de viva voz y las autoridades de la misma tomaban nota (en 1873, se cambió el voto oral por el escrito, pero seguía siendo público). Los resultados estaban disponibles ni bien finalizaba el comicio, sin demoras. Y nadie podía sospechar que se había cambiado su voto, ya que todo estaba a la vista. Pero llegó el secreto, y cambió de raíz el sistema de votación.

Estamos a más de cien años de ese cambio, y celebramos que gracias a él pudimos finalmente tener elecciones libres y justas, aun tolerando ciertas demoras en conocer los resultados. Y también, sabemos que es posible que algunos votos sean adulterados, pero también podemos buscar la forma de mejorar el sistema (y la fiscalización) para minimizar esos casos.

Hoy se nos propone votar usando computadoras. Con la promesa de tener resultados provisorios más rápidamente, con la esperanza de que sea más difícil adulterar el resultado de la votación (esperanza que muchas veces radica en una forma de pensamiento mágico).[9] A cambio, la posibilidad del votante de cerciorarse de que su voto es secreto se ve severamente comprometida. ¿Puede alguien que esté bajo presión correr el riesgo de creer en la palabra autorizada de un grupo de auditores que le asegura que todo se hace correctamente? ¿Debe un ciudadano confiar en una élite al realizar el acto vital y primigenio de una democracia republicana? Claramente, no.

---

9 "Magia electrónica", 01/08/2015, https://blog.smaldone.com.ar/2015/08/01/magia-electronica/

Sobre cómo mejorar el sistema

El sistema actual tiene problemas, eso es evidente. Pero en la búsqueda de la solución, no debe debilitarse el pilar del secreto del voto. ¿Hay robo de boletas o boletas falsas en el cuarto oscuro? Usemos boletas únicas –como la mayoría de los países del mundo–, papeles con grillas donde aparezcan todas las opciones, que sean retiradas de la mesa de votación por el votante (lo que también elimina el "voto cadena"). ¿Alguien duda sobre la posibilidad de boletas marcadas? Que la boleta única sea retirada por el ciudadano de una pila colocada al lado del presidente de mesa, eligiendo la que más le plazca. ¿Se adulteran boletas en el escrutinio? Pensemos en medidas de seguridad para evitarlo (no, ninguna funcionará sin fiscalización, por más que usemos los sistemas electrónicos más rebuscados). ¿Las actas confeccionadas manualmente tienen errores o resultan ilegibles? Usemos sistemas de impresión dispuestos en los centros de votación. ¿El escrutinio provisorio parece una "caja negra" en donde pueden alterarse los resultados? Usemos los medios que proveen la informática y las telecomunicaciones para abrirlo a la ciudadanía, de modo que todos podamos controlar, desalentando por lo tanto las manipulaciones.

En la mejora del sistema de votación, debemos buscar más transparencia. Debemos dar más control al votante sobre su voto, y no menos. Interponer entre el votante y su voluntad un elemento tan opaco (u oscuro) como una computadora va exactamente en el sentido opuesto: no ofrece transparencia, necesita auditorías; no brinda confianza, la requiere.

La experiencia mundial así lo evidencia: el uso de computadoras para emitir el voto, luego de más de cuatro décadas de investigación, desarrollo y pruebas, está en franco retroceso en la inmensa mayoría de los países. Actualmente, solo en Brasil, Venezuela, India y la mitad de Bélgica se vota usando computadoras. En los EE. UU., pionero mundial del uso de máquinas –inicialmente mecánicas, luego electrónicas– para votar, cada vez son más los estados que se vuelcan al uso de boletas de papel. En 2010, Israel descartó el uso de

un sistema muy similar al de la "boleta única electrónica". Finalmente, en el caso extremo de países como Alemania, los Países Bajos, Irlanda y el Reino Unido, después de probar en mayor o menor grado alternativas de este tipo, erradicaron completamente las máquinas.

Es particularmente esclarecedor el fallo de 2009 de la Corte Constitucional de Alemania, que declaró inconstitucional el uso de computadoras para votar (el énfasis es agregado):

> 1. El principio de la publicidad de la elección del artículo 38 en relación con el art. 20 párrafo 1 y párrafo 2 ordena que *todos los pasos esenciales de la elección están sujetos al control público*, en la medida en que otros intereses constitucionales no justifiquen una excepción.
>
> 2. En la utilización de aparatos electorales electrónicos, *el ciudadano debe poder controlar los pasos esenciales del acto electoral y la determinación del resultado de manera fiable y sin conocimientos técnicos especiales*.[10]

La garantía del secreto del voto es esencial. Es vital fortalecerla, para seguir preservando la máxima de Sáenz Peña, y que un voto comprado no pueda transformarse en un voto vendido, si el votante así lo dispone.

---

10 Sentencia 2 BVC 3/07 - 2 BVC 4/07, Corte Constitucional Alemana (traducción de Manfredo Koessl).

Vot no[1]

Nicolás D'Ippolito

Hablemos de las elecciones. Hablemos de la boleta única electrónica.

Sin preámbulos ni entrada en calor, hablemos de la posibilidad de que alguien pueda manipular las máquinas que usaríamos para votar. Podemos empezar por prestar atención al siguiente fragmento de código:

```
[…]
    read_unlock(&tasklist_lock);
    if (flag) {
    retval = 0;
    if (options & WNOHANG)
```

1 Este artículo fue publicado originalmente en el sitio *El Gato y la Caja*. Se puede leer el original que incluye algunas imágenes y videos en https://elgatoylacaja.com.ar/vot-no/

```
    goto end_wait4;
    retval = -ERESTARTSYS;
    if (signal_pending(current))
    goto end_wait4;
    schedule();
    goto repeat;
    }
   if ((options == (__WCLONE|__WALL)) && (current-
>uid == 0))
    retval = -EINVAL;
   else
    retval = -ECHILD;
   end_wait4:
    current->state = TASK_RUNNING;
    remove_wait_queue(&current->wait_chldexit,&wait);
    return retval;
   }
```

Es importante verlo detenidamente, sé que parece tedioso pero vale la pena el esfuerzo. Acá va de nuevo:

```
   […]
    read_unlock(&tasklist_lock);
    if (flag) {
    retval = 0;
    if (options & WNOHANG)
    goto end_wait4;
    retval = -ERESTARTSYS;
    if (signal_pending(current))
    goto end_wait4;
    schedule();
    goto repeat;
    }
   if ((options == (__WCLONE|__WALL)) && (current-
>uid = 0))
    retval = -EINVAL;
   else
```

```
 retval = -ECHILD;
end_wait4:
 current->state = TASK_RUNNING;
 remove_wait_queue(&current->wait_chldexit,&wait);
 return retval;
}
```

¿Qué es lo importante de este código? Que no es uno, son dos distintos, con una pequeña diferencia: uno de ellos tiene un signo '=' de menos. Es la única diferencia, dos miserables rayitas, pero con una implicancia no menor: si el segundo estuviese corriendo en una computadora, esta podría ser hackeada con facilidad. Se trata de un caso real del año 2003, de código que se encuentra en la parte central del sistema operativo Linux.[2] La diferencia entre la versión correcta y la que te hace sonar es tan sutil que es muy difícil de detectar, incluso por expertos (para ser riguroso, este caso se detectó con facilidad porque se trató de una modificación a un código ya existente y hay herramientas que muestran solo aquellas líneas que cambiaron, que en este caso eran solo dos, cuando hay que auditar una pieza de software desde cero no se cuenta con esa ventaja).

Me adelanto a la objeción: si fuera tan difícil, ¿cómo saben las empresas que venden software que sus productos no tienen fallas? La respuesta es muy sencilla: no lo saben. Y no se trata de que en su ansia desmedida por apropiarse de la renta saquen productos a medio cocinar. Bueno, a veces un poquito sí, pero hay dificultades mucho más de fondo.

Seguro es el que probó y confió

Ahora, podríamos probar con probar, ¿no? Es decir, si uno quiere saber si una pieza de software falla en algún caso,

---

2 Felten, Ed. "The Linux backdoor attempt of 2003", 09/10/2013, http://freedom-to-tinker.com/2013/10/09/the-linux-backdoor-attempt-of-2003/

puede probarla y con eso alcanza, ¿no? No, la verdad es que con probar no alcanza. El testing es la disciplina informática encargada de probar una pieza de software buscando incrementar la confianza que se tiene en que opera como debe. Funciona así: uno prepara una batería de casos de prueba, que son descripciones paso a paso de qué hacer con el sistema, y compara el resultado obtenido con el esperado. Si no son iguales, acabamos de encontrar un defecto (lo que coloquialmente se llama 'un bug').

Por otro lado, si sí lo son, la única garantía que tenemos es que esa interacción (y no otra, y mucho menos todas) funcionó bien la vez que la probamos, pero tampoco es que estamos tan seguros. Aun si corremos otra vez exactamente la misma secuencia, este segundo intento podría fallar porque no sabemos si el programa en cuestión tiene en cuenta alguna 'variable invisible', como por ejemplo la hora de la computadora, y entonces se comporta de una forma cuando esa variable es una (digamos, a las 9:13 de un martes), y de forma distinta en otra (por ejemplo, a las 4:12 de la madrugada del sábado). El que no se comporte distinto a las 4:12 del sábado, que tire la primera piedra.

Aun si tuviésemos el código y pudiésemos mirar todas las variables involucradas, las alternativas crecen exponencialmente y los caminos posibles a probar son millones de millones. Es decir, el testing es un paso fundamental para asegurar la calidad del software, y cuando encuentra un defecto, hay que arreglarlo; pero el testing nunca puede asegurar la ausencia de defectos.

Existen métodos automáticos que también ayudan a aumentar la confianza en que el software funcione como se espera. Algunos son muy buenos, pero tampoco son infalibles. La cosa se complica aún más si estamos haciendo testing de seguridad, ya que en ese caso el comportarse correctamente implica que no solo haga lo que tiene que hacer, sino que no haga nada 'extra'. Un ejemplo puede ser el caso del acceso a un home banking: no solo debe dejarme entrar solamente con la contraseña correcta, sino que siempre

debe transportarla por la red de manera encriptada y un largo etcétera de requisitos que hacen a la fortaleza y seguridad del sistema.

Pero hay más: no solo debe cumplir con estos requisitos, sino que no debe tener ningún tipo de agujero de seguridad, de esos que aprovechan los virus y los hackers para subvertir un sistema y hacer que sucedan cosas no contempladas. En un sistema informático, es muy, muy difícil encontrar fallas sutiles (a modo de ejemplo, un bug de seguridad en un software de código abierto muy usado estuvo presente 20 años hasta que fue hallado u otro que se detectó hace pocos días y estuvo latente por 11 años y presente en las máquinas con las que se votó en la CABA), y ni hablar de aquellas que son introducidas a propósito con la intención de que no puedan hallarse. Valga como ejemplo el bug introducido intencionalmente en el año 2006 en la especificación de (prepárense que parece chino lo que sigue, pero es algo importante) el generador de números al azar 'Dual_EC_DBRG', que es una parte central de muchos algoritmos criptográficos. Posteriormente, varios fabricantes implementaron el estándar viciado en sus productos y por ende muchísima información sensible que debía ser protegida por mecanismos criptográficos quedaba al desnudo para el autor del bug, que muchos sospechan que se trataba de la NSA. El incidente recién salió a la luz pública en el año 2013.

Algo que sabemos hace mucho en el mundo del software es que uno no puede tener garantías de que no hay fallas, y a lo que debe apuntar es a tener un muy alto nivel de confianza en que el sistema en cuestión funcione como se espera.

¿Qué tan grave es que falle el software? Bueno, si falla Tinder, tal vez nuestros genes no se propaguen (quién te dice, terminamos haciendo un bien a la humanidad). Ahora, si falla un marcapasos, uno pensaría que es bastante más grave. Pero, ¿y si el software altera o permite alterar un resultado electoral? Como el marcapasos, pero de escala país. A eso se lo conoce como la *criticidad*, es decir, qué tan graves son las consecuencias de que falle un sistema.

Cuando se trata de software crítico a lo que debe apuntarse es a hacer nuestro mejor esfuerzo para disminuir la chance de que ese software tenga fallas. Cabría preguntarse por qué se usa software en esos casos si no puede garantizarse que sea seguro. La respuesta es simple: porque las otras alternativas que podrían cumplir las mismas funciones o bien no existen o también pueden fallar.

Tener un alto grado de confianza en un sistema tan crítico como el que interviene en una elección requiere de mucho tiempo de trabajo por parte de un grupo de expertos, que utilizará técnicas como inspección ocular, revisión entre pares, testing, análisis estático y dinámico de código, penetration testing (no relacionado con Tinder) y un largo etcétera durante un periodo prolongado de tiempo. Los hallazgos de ese trabajo realimentarán el proceso de diseño y programación del sistema, y el proceso de prueba deberá recomenzar. Pero, ¿qué pasa en el caso de una elección? ¿Es posible que todos estos controles no sean suficientes? Sí.

Para nosotros que lo miramos por TV

Para entender por qué, imaginemos el próximo proceso electoral de nuestro país: una compra así de grande debe hacerse por licitación, supongamos que se hace mañana, que procede sin dificultades y se evalúa en tiempo récord.

[Pausa para recuperarse de la risa]

El 1° de enero de 2017 la empresa concesionaria termina por completo de desarrollar los sistemas que intervendrán en la elección, los prueba, los analiza y determina que funcionan correctamente. No estamos hablando de desarrollar una app chiquita; se trata de un sistema muy grande, que incluye mucho código desarrollado por la propia empresa, mucho código desarrollado por terceros, e incluso un sistema operativo o parte de él (que puede tener fallas como

las que describimos al comienzo del artículo). Todas y cada una de esas partes deben chequearse profundamente porque funcionan de manera encadenada y el resultado final puede alterarse en cualquiera de ellas. En definitiva, el sistema entero es tan fuerte como la parte más débil de la cadena.

Ese 1° de enero, ya curada la resaca, expertos de todos los partidos se reúnen y analizan el sistema utilizando todas las técnicas que mencionamos anteriormente. El sistema completo a probar es muy complejo, dado que contiene hardware (lo que se puede patear) y software (lo que solo se puede putear), así que les toma 6 meses. Menos tiempo, no es realista; más tiempo, se dificulta llegar a agosto con las máquinas repartidas por los más de 3 millones de km cuadrados de nuestro territorio. Entonces se juntan y en un éxtasis de felicidad brindan porque todas las fallas que fueron encontrando se fueron arreglando (lo cual solo significa que no encontraron más fallas, no que no existan).

La primera pregunta es: ¿cómo saben que todos auditaron el mismo sistema? Eso es fácil de resolver con el software porque uno puede calcular una firma digital del código del sistema, y si las firmas coinciden es que auditaron el mismo software. ¿Y el hardware? Bueno, no existe tal cosa como la firma digital del hardware, así que realmente no hay forma de saber que probaron con el mismo hardware, y eso es importante porque lo que determina qué va a pasar es la combinación de hardware y software. Y sí, se pueden poner "virus" por hardware.

Pero supongamos que decidimos pasar por alto ese "detalle" y, en un acto de fe ciega, suponemos que todas las computadoras que se van a usar en la elección fueron bendecidas por Santo Tomás de los Pines en persona y por ende suponemos que el hardware simplemente ejecuta el software en forma fiel, sin interferir con su funcionamiento (insisto con esto: en un acto de fe). ¿Cómo sabemos que el software que se va a ejecutar es el que fue auditado? Deberían reunirse todos, todos, todos, frente a otra de esas computadoras bendecidas y compilarlo ahí mismo (*compilar* es el proceso por el que se

pasa de un texto escrito en un lenguaje de programación a esa secuencia de ceros y unos llamada código de máquina, que es lo único que "entiende" una computadora realmente). De nuevo, necesitamos otro acto de fe para ignorar el artículo de Ken Thompson, laureado en 1984 con el Premio Turing (aka "el Nobel de la Computación"), llamado "Reflections on Trusting Trust", que explica cómo el propio compilador puede ser saboteado para, a partir de un programa sin problemas, producir código de máquina malicioso.[3]

Supongamos que también ignoramos eso, así como el trabajo posterior que lo muestra en la práctica. Tenemos nuestro código de máquina compilado delante de todos, que suponemos que no tiene trampas. Calculamos una firma digital de ese código de máquina y se la pasamos a todos nuestros fiscales. Y ojo acá, que cabe recordar que ya venimos acumulando dos actos de fe, uno por el hardware, otro por el compilador.

Llega el día de la elección, viene el empleado del correo con una de esas máquinas que por acto(s) de fe suponemos que no tienen problemas. Trae también su CD o pendrive con el código de máquina que es lo que define qué pasará realmente con ella, y cada uno de los fiscales partidarios chequea con su computadora (que tienen, porque la VAN a necesitar, así que asumimos que hay una computadora para CADA fiscal) si la firma digital de ese CD o pendrive coincide con el que fue compilado delante de todos. Esto es absolutamente indispensable, porque si los fiscales no pueden corroborar individualmente que el software que se instala en cada máquina es el auditado, no solo existe la posibilidad real de que se instale otro, sino que además se deja abierta una puerta para que cualquiera disconforme con el resultado lo atribuya a una adulteración y tenga un punto muy fuerte a su favor.

---

3 El artículo en inglés se puede leer en esta página: http://dl.acm.org/citation.cfm?id=358210

Todo esto supone además que no hay que hacer ninguna modificación de último momento (como que la justicia autorice algún cambio en las listas o en la forma de presentarlas, algo que es muy usual), porque habría que repetir todo el proceso de nuevo, ya que cambia el código fuente, el código de máquina y la firma digital.

Nada puede malir sal

¿Qué podría pasar si las máquinas de votación estuvieran "comprometidas"? La verdad, de todo. Recordemos que, en el formato 'boleta electrónica', el ciudadano elige a sus candidatos y la máquina debe grabar su elección de forma digital y además imprimirlo en formato legible. Una máquina comprometida o adulterada podría imprimir al candidato A en letras y grabar digitalmente al B.

No tiene que hacerlo siempre, que sería muy obvio, puede hacerlo en una cantidad estadísticamente pequeña de casos, lo suficiente como para asignarle una banca de más o de menos a algún partido, o definir un ballotage muy parejo para una presidencia (pongámosle un 51 a 49 hipotético, o recordemos también el referéndum en Colombia[4] donde el No ganó con 50,2% de los votos).

Si de variaciones estadísticas se trata, también podría pasar que el orden al azar en el que aparecen los candidatos no sea tan al azar, dándole prevalencia a alguno. No vamos a hacer un listado exhaustivo, pero analicemos un poco más.

Unos investigadores independientes reportaron un defecto en el sistema usado en la CABA para las elecciones para Jefe de Gobierno de 2015: permitía cargar varios votos a la vez,

4 Se refiere al referéndum sobre las FARC. Este artículo amplía el tema mencionado: "Referéndum con sorpresa: los colombianos rechazar el acuerdo de paz con las FARC", Clarín, 03/10/2016, http://www.clarin.com/mundo/referendum-sorpresa-colombianos-rechazan-farc_0_r1stzByo.html

algo que ninguna de las auditorías oficiales había notado.[5] Otro investigador descubrió un manejo poco seguro del mecanismo de encriptación utilizado, lo que permitía que cualquiera mandara al centro de cómputos resultados como si fuesen oficiales. Lo reportó antes de las elecciones y por supuesto que fue automáticamente respetado y tratado con cuidado… O no: fue allanado y enfrentó un proceso judicial que duró casi un año[6] (así como al pasar, durante ese proceso se determinó que los servidores de la empresa que brindó el servicio habían sido hackeados), con altos costos, hasta que finalmente la justicia determinó que no había cometido ningún delito (y hasta que había dado una genuina mano identificando los problemas). Porque si hay algo que querés cuando reportás un bug en un sistema público crítico es que te traten como un peligroso delincuente y te secuestren todos los aparatos electrónicos, incluyendo compu, laptop, Kindle, y una licuadora que parece que miraba fijo a uno de los gendarmes.

Pero, si es electrónico, tiene que ser fantástico

Una objeción que se escucha con frecuencia es que está previsto el escrutinio manual. Analicemos esta posibilidad basándonos en los datos duros del informe final de la Defensoría del Pueblo de la CABA sobre la elección para Jefe de Gobierno de 2015. Según este informe, "una vez cerrada la mesa, el 83,9% de los presidentes pudo realizar el escrutinio sin inconvenientes. Durante el conteo de votos, solo el 10,1% de las mesas contó con fiscales que realizaron algún reclamo". Esto significa que hubo cerca de 730 mesas con

---

5 Cf. Video "Multivoto: sumando múltiples votos con una boleta en el sistema vot.ar", https://www.youtube.com/watch?v=CTOCspLn6Zk

6 Para ampliar sobre el caso de Joaquín Sorianello, se puede leer este artículo: http://www.clarin.com/politica/allanan-detecto-vulnerabilidades-sistema-electronico_0_HkBRiUKwml.html

reclamos. A 300 votantes por mesa, hay unos 219000 votos en cuestión, muy por encima de los 54000 que definieron la elección en CABA y peligrosamente cerca de los 300000 votos de diferencia que definieron el ballotage presidencial de ese mismo año. De ese informe surge también que un 26,2% de los votantes dijo no haber verificado que el voto impreso coincidiera con lo que había elegido.

Pero además, aun en el caso en que todas las mesas electorales corroboraran el escrutinio electrónico con uno manual, el manual es solo corroboración de una planilla que se graba digitalmente en otra boleta electrónica. De nuevo, un software malicioso podría hacer que la grabación tenga cifras adulteradas incluso cuando la propia máquina las siga mostrando como correctas. O tal vez la manipulación podría hacerla la máquina que lee la tarjeta y manda la información a través de Internet hacia el centro de cómputos (que a su vez podría tener software adulterado o hackeado como el de CABA en 2015). No sé cómo vienen ustedes, pero a esta altura ya perdí la cuenta sobre la cantidad de saltos de fe.

Memoria y "países serios"

El pueblo argentino se ganó el voto universal, secreto y obligatorio en cuotas. Primero nos ganamos el voto (de entrada solamente los varoncitos, aunque ellas conquistaron la universalidad un par de cuotas más tarde), varias dictaduras nos lo sacaron y hubo que reconquistarlo. En el medio de esas peleas, conquistamos el voto secreto, y lo consagramos en la Ley Sáenz Peña.

Entonces teníamos la posibilidad de que nadie supiera a quién votaste, para que no pudieran chantajearte, presionarte, comprarte o vengarse de vos si no les gustaba tu decisión. Esto se manifiesta de manera muy clara cuando tenemos la posibilidad de poner nuestro voto en un sobre idéntico a todos los sobres para después abrir la urna y contar (y sí, hay maneras de manipular y de romper el secreto de voto, pero

son fácilmente identificables y auditables por ciudadanos comunes).

Hay que tener memoria, algo que las computadoras también tienen. Justamente el tema de la memoria es central en el argumento de la Corte Suprema de Alemania que, en el año 2009, prohibió el uso de urnas electrónicas porque contradice el principio de que todos los pasos de la elección estén sometidos al escrutinio público sin requerir conocimientos técnicos especiales.

Si pudiera elegir un solo párrafo para ser recordado de todo este texto (que intenta ser exhaustivo respecto de las múltiples aristas a considerar en la adopción o no del voto electrónico y sus variantes), sería éste: si dependemos de un proceso técnicamente inaccesible para la enorme mayoría de nosotros (salvo los expertos en desarrollo de sistemas de votación electrónica), la transparencia del sistema para el ciudadano común desaparece.

Con el voto electrónico y sus variantes, a la democracia la vemos pasar, la miramos por TV. Nos cuentan y tenemos que creer o reventar. El pilar de nuestra construcción democrática, la elección, se transforma en algo que no entendemos, que no podemos auditar. No es un detalle menor que el voto sea secreto. Es esencial y nadie nos lo regaló, hubo que luchar mucho para conseguirlo. Con el voto electrónico y sus variantes, puede dejar de serlo. Lo que es peor aún, no sabemos si es o no secreto, y sembrar esa duda (que se vuelve razonable porque el sistema es tan opaco que no hay forma de saber la verdad), alcanza para que alguien pueda manipular nuestra decisión. El voto no solamente tiene que SER secreto, sino que tiene que LUCIR secreto, para poder ser ejercido sin presiones.

De imprentas e impresoras

El sistema actual no es perfecto: es cierto que es problemático y costoso distribuir las boletas a todos los cuartos oscuros,

y que sería muy bienvenida una alternativa superadora a semejante desafío logístico, especialmente para los partidos chicos. Pero superadora de verdad, no solo aparentemente. Si vamos a informatizar, pensemos en lo que pasa después de votar, desde hacer un conteo asistido de los votos hechos en papel a cosas mínimas como disponer de un procesador de texto y una impresora en los cuartos oscuros para que las actas no sean manuscritas y haya menos errores de transcripción.

Muchas veces se revolea el argumento de que las máquinas de votación son solamente impresoras. Es un argumento casi gracioso porque las impresoras de hoy en día son solamente otro tipo de computadoras y, como tales, también tienen memoria. Y pueden usar esa memoria para registrar que, por ejemplo, el primer votante votó por A, el segundo por B, el tercero por A de nuevo, y así siguiendo. Con el simple expediente de ir contando, todos los fiscales partidarios pueden saber quién votó primero, quién segundo, etcétera. No solo los fiscales, basta con poner a un chabón a fumar en la puerta del cuarto oscuro. Es decir, no alcanza con que el sistema no manipule los resultados, también hay que garantizar que no registre información de más.

Y la verdad es que en este caso hace falta poca memoria, o casi ninguna: en cada cuarto oscuro votan unas 300 personas; ese número se codifica con solo 9 bits.

Si no te resulta obvio que el número 300 se codifica con 9 bits, es un claro ejemplo de cómo el sistema que estamos discutiendo también te dejó afuera a vos, una persona probablemente educada, curiosa e informada, pero que no tiene conocimientos específicos sobre computación. Qué loco pensar que con esas mismas condiciones sí podrías auditar todo el proceso de voto en papel: saber leer, ser curioso y educarte respecto del proceso de fiscalización (algo que demora minutos).

Decíamos que alcanza con 9 bits, 9 puntitos escondidos en cualquier parte de la boleta en papel para saber a quién votó cada persona. Si alguien va contando en qué orden vota cada uno de los electores, luego, cuando recuperan las boletas en

papel, se miran esos 9 puntitos mínimos, escondidos con algo de cautela, tal vez en el borde de una letra, tal vez simulando ser una mancha de tinta, y se puede reconstruir a quién votó cada elector. ¡En tu cara, Sáenz Peña!

Comparando

El sistema electoral actual no es perfecto y tiene mucho para mejorar. Pero es mucho mejor de lo que se nos quiere hacer creer repetidas veces. Si una fuerza política quiere gobernar una ciudad debe concitar las voluntades de la mayor parte de los electores de la ciudad, pero el requisito previo es que tenga un núcleo de personas con un nivel mayor de adhesión, realmente entusiasmados por la propuesta, que estén dispuestos a ser fiscales durante un día. ¿Con qué requisitos? Los básicos: prestar atención, saber leer, sumar y restar, condiciones que en líneas generales cualquier adulto puede cumplir. Sería razonable que las fuerzas políticas que tienen una ambición mayor, como la de gobernar una provincia, tuvieran una cantidad de entusiastas proporcional al tamaño de la provincia. Si no, es muy difícil pensar que la van a poder gobernar. El mismo razonamiento cabe si quieren gobernar un país. Por supuesto que no es fácil, pero gobernar tampoco lo es. Si no podés resolver el problema de conseguir veinte fiscales para ser intendente de tu ciudad, difícilmente puedas resolver los problemas que conlleva la propia intendencia, donde son muchas más las voluntades que deben alinearse, durante mucho más tiempo que un par de domingos cada dos años. Lo mismo si querés gobernar un país.

Por otra parte, es poco verosímil y hasta peligroso que una fuerza política acepte dejar la máquina de votación sin supervisión, con lo que la implementación de mecanismos electrónicos tampoco elimina la necesidad de fiscales.

Para los fiscales, el sistema actual podría mejorarse en varios puntos, pero el hecho de poder entrar por la web y ver si el telegrama escaneado tiene tu firma y si la planilla

electrónica coincide con lo que está escrito a mano y con tu copia del acta es un punto de control muy fuerte.

Dada la propuesta actual de voto electrónico, con tener fiscales no alcanza, porque en definitiva los puntos de control establecidos de nada sirven si se pierde el secreto del voto, si lo que se graba en la boleta no refleja la voluntad del elector en todos los casos, o si luego esa información es nuevamente volcada a otra computadora que puede manipularla en el proceso.

No es menor decir que este análisis no parte de ser un romántico de los viejos tiempos o un férreo opositor a la ciencia y la tecnología. Lejos estoy de serles fóbico o de no comprenderlas. Es más bien lo contrario en este caso: entender cómo funciona la tecnología digital nos da herramientas para poder mirarla con ojos críticos. Justamente por eso entendemos sus limitaciones, como lo hacen casi todos los países desarrollados (para nada tecnofóbicos), que siguen votando en papel.

De hecho, si lo que se busca es boleta única, existe la boleta única en papel: en un mismo cacho de árbol tenés a todos los candidatos de todos los partidos y le ponés una cruz a los que prefieras (la única dificultad es que hay que explicarles a los adolescentes que se elige solo con una cruz y no vale usar otros emoticones).

Decía más arriba que con la boleta electrónica la transparencia se pierde, y es importante recalcar que no reaparece si, en lugar de implementarse a las apuradas, se hiciese con tiempo suficiente.

El sistema está intrínsecamente viciado porque el piso mínimo necesario para entender el proceso electoral electrónico, auditarlo y participar de su control, se vuelve prácticamente inalcanzable. Pasa de requerir habilidades que se adquieren en la escolaridad básica a volverse una discusión de expertos, cerrada, críptica, y por ende, excluyente.

Somos los ciudadanos y ciudadanas comunes, los que armamos ese nosotros bien grande que trasciende lo que nos aúna y lo que nos separa, los que queremos poder votar de

forma secreta y segura, y que nuestro voto se escuche. Que se escuche cristalino, sin intermediarios, dudas o mugre.

Que se escuche exactamente como lo manifestamos, aun cuando el resultado no nos guste, pero sabiendo que genuinamente nos representa.