lanacion.com.ar

Algunas reflexiones sobre el voto electrónico

Sábado 11 de julio de 2015

Ésta es una de las columnas más extensas que he publicado en LA NACION. Pero prefiero pecar por exceso que por defecto (y eso que corté párrafos completos). El tema del voto electrónico tiene docenas de facetas, es extremadamente técnico y está altamente politizado. Es el caldo perfecto para las simplificaciones y las verdades a medias. He querido evitar ambas porque lo que está sobre la mesa es uno de los procesos más críticos de una democracia occidental: los comicios.

Por completud, ya que sería imposible tratar todos los matices aquí, quiero destacar un meticuloso artículo de Enrique Chaparro y el que Javier Smaldone publicó en Perfil.com. Smaldone (@mis2centavos) ha sido, junto con Beatriz Busaniche (@beabusaniche), de la Fundación Vía Libre, dos de los críticos más activos del voto electrónico.

Vía Libre, con el apoyo de la Fundación Heinrich Böll, publicó en 2009 el libro "Voto electrónico, los riesgos de una ilusión", que puede descargarse aquí: http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf

A los coletazos legales y políticos directamente relacionados con el sistema que se estrenó en Buenos Aires el domingo último se sumaron las repercusiones en el extranjero. Cubrieron el tema Der

Spiegel, BoingBoing, TechDirt y ArsTechnica.

Por último, y para atajar de antemano la falacia de afirmación del consecuente, mis reservas respecto del voto electrónico no significan que ignore los defectos del voto en papel. De hecho, y como se verá enseguida, los conozco en primera persona.

***

Fui autoridad de mesa en 4 ocasiones. Durante las PASO y las elecciones presidenciales de 2011, y nuevamente en 2013. Aprendí mucho, sentí que hacía un aporte a la República, y vi cosas. Muchas cosas. Desde fiscales que apenas sabían leer y escribir hasta delegados de la autoridad electoral desbordados. Hoy sé que aprendí algo más: no se puede opinar sobre el voto electrónico sin haber pasado por esa larga y extenuante jornada en la que tenés los 5 (o 6) sentidos puestos en que cada voto sea secreto y aparezca asentado en las planillas. Y en que nadie haga trampa, claro. Con todo y la rusticidad de la boleta de papel y el conteo manual, tengo la impresión de que esta tarea es, todavía, cosa de humanos, no de máquinas.

Pero lo entiendo. En primera instancia es difícil no estar de acuerdo con los que defienden el voto electrónico. Es más barato para los partidos chicos, más eficiente y más a tono con los tiempos. Para el ciudadano, según oí decir a muchos el domingo, es "más rápido y práctico".

El único problema es que el voto electrónico no es electrónico. Es informático.

La radio y el velador

La diferencia entre eléctrico, electrónico e informático puede

parecer una sutileza semántica. No lo es.

Empecemos por lo más simple. El velador en tu mesa de luz es un dispositivo eléctrico, porque no hay ningún componente activo, excepto la lamparita en sí, que es, escasamente, un filamento que se calienta hasta ponerse incandescente cuando circula corriente por él.

En cambio, una radio a transistores es electrónica. En su interior funcionan circuitos compuestos por resistencias, transistores y capacitores. Su función es mucho más compleja que la de calentarse y brillar; sintoniza señales, las amplifica y las envía al altavoz.

La informática es electrónica por definición, porque nuestras computadoras -al revés que el ábaco o la inconclusa máquina de Babbage- no son mecánicas, sino que usan circuitos con (de nuevo) transistores, resistencias, capacitores, etcétera. La diferencia con la radio a transistores es que en las computadoras hay, además, un componente muy especial, el microprocesador, también conocido como "cerebro electrónico". ¿Y por qué esto es diferente de una radio a transistores?

Primero, porque los cerebros electrónicos pueden ejecutar una tarea mucho más amplia y poderosa que sintonizar señales o amplificarlas. Su función es hacer cálculo numérico y evaluar proposiciones lógicas.

Pero, además, la radio nunca va a poder hacer otra cosa que sintonizar estaciones y pasar el sonido por el altavoz. No podés programar su electrónica para que en lugar de captar AM y FM haga cálculo numérico. Opuestamente, los cerebros electrónicos son, por definición, programables. La única tarea para la que han sido diseñados es para que alguien los programe para hacer algo.

Suena absurdo, porque durante 100.000 años diseñamos nuestras herramientas pensando en su función y no al revés. Pero este concepto, el de una herramienta que es todas las posibles herramientas, revolucionó el mundo en los últimos 30 años.

Por eso, tu computadora o tu smartphone pueden ser usados para un número no sólo muy grande de tareas (WhatsApp, Twitter, escribir, jugar, dibujar el plano de una casa, crear películas en 3D, sacar fotos, navegar por GPS, hablar por teléfono), sino que ese número no tiene techo. Si la tarea puede expresarse por medio de algoritmos, entonces puede programarse.

Puesto que la matemática y la lógica son destrezas propias del cerebro humano, solemos decir que un dispositivo programable es "inteligente". Lamentablemente, esto es una exageración. Porque también se puede obligar a la computadora a hacer algo pernicioso o francamente insensato; es la función, por ejemplo, de la mayoría de los virus informáticos. Nunca hubo virus para radios o veladores, ¿o sí? No, porque no son dispositivos programables.

La delgada línea de código

Ahora, ¿cómo se instruye a un cerebro electrónico para que haga algo? Mediante los programas, el software. Existe un axioma respecto del software, uno que se prueba cierto cada día: es vulnerable a ataques informáticos.

Sólo durante junio y sólo desde el Computer Emergency Readiness Team de Estados Unidos (US-CERT) se emitieron 134 advertencias sobre vulnerabilidades muy graves en el software de, entre otros, Adobe, Apache, Blue Coat, Cisco, Dell, FusionForge, Google, IBM, Microsoft, Mozilla, SAP, Ubuntu, VMWare, tecnologías de cifrado (OpenSSL) y lenguajes de programación. Extrapolando, serían más de 1600 al año. Esto, sin contar las fallas

menos críticas.

Las vulnerabilidades no son la excepción, sino la regla, y los programas pueden ser inseguros no sólo por estar mal hechos, sino porque una función normal, lícita, podría explotarse con fines maliciosos. Como me explicaron hace varios años en la sede de Microsoft, en Buenos Aires, algunas vulnerabilidades son como las ventanas; todos queremos ventanas, pero si son de fácil acceso desde el exterior, las enrejamos. Hace 30 años, no. Hoy, sí.

O sea que sí, las vulnerabilidades son también una cuestión de fechas.

El software habita en todos los rincones de una computadora, tablet, smartphone y prácticamente cualquier cosa que use corriente eléctrica. El sistema operativo es software. La aplicación que se ejecuta (para escribir o para votar) es software. Los controladores de dispositivos -indispensables, por ejemplo, para mostrar algo en una pantalla o para imprimir- son software. Los jueguitos, los virus y hasta las fuentes tipográficas son software. Es más: cuando una computadora arranca lo primero que hace es ejecutar un software conocido como POST (por Power On Self Test), que está embebido en el hardware. Sin software, sin código ejecutable, una máquina es un montón de plástico, cobre y silicio, inerte e inútil.

Conclusión: una computadora o no arranca o es vulnerable. No hemos alcanzado todavía el estado del arte para evitar esta disyuntiva de hierro que en el ambiente informático se conoce desde siempre; de allí que gran parte de la comunidad tecnológica se haya opuesto tan frontalmente al voto con computadoras. Conocen bien estos sistemas y saben de su fragilidad.

Opaco por definición

Entre las pocas cosas que no tienen código ejecutable se encuentran los documentos de texto plano o puro. Están compuestos sólo de texto. Pero aquí ingresa otro dilema de la computación. No hay -ni podría haber- en estas máquinas ninguna transparencia. Todo es opaco. ¿Por qué? Porque para poder visualizar (o imprimir) incluso un inocente documento de texto puro hace falta ejecutar un programa.

Dicho de otra manera, no hay modo de acceder a ningún dato en una computadora sin pedirle al cerebro electrónico que ejecute una serie extensa, compleja e invisible de instrucciones. Así que el hecho de que un TXT o un JPG no contengan código ejecutable no resuelve el pecado original de todo sistema informático: es opaco por definición.

Esto es porque en una computadora no hay ni letras ni colores ni sonido ni candidatos, sino sólo números. Extensas cadenas de unos y ceros que necesitan un sistema de hardware y software para mostrarse como algo inteligible. O para mostrar lo que el programador decidió que veamos. Es, en rigor, lo opuesto a la transparencia.

El grado cero de la democracia

Cuando se debate sobre el voto electrónico suele hacerse hincapié en la posibilidad de que facilite el fraude. Pero aunque éste sería el escenario más temido, hay un problema más grave, más insidioso y más escurridizo. Porque, a fin de cuentas, el voto ya es en gran medida informático hoy. De otro modo no tendríamos los resultados a las 9 o 10 de la noche.

La cuestión es que esa fracción del proceso que todavía se tramita con papel (elegir una boleta, ponerla en un sobre y colocarla dentro de una urna, contarlos y asentarlos a mano) es la salvaguardia de

todo lo que luego harán los centros de cómputo. Se podrá después hackear computadoras o podrá haber error humano, pero allí están las urnas y sus boletas, más las planillas que las autoridades de mesa y los fiscales llenaron de puño y letra. Sé que suena antiguo y poco eficiente, sobre todo después de haber votado con una computadora. Lejos de eso.

Al revés que los bits, este polímero natural que usamos desde hace siglos no puede fraguarse sin que se note, y su contenido se puede fiscalizar a simple vista, sin que medien artilugios electrónicos. Nuestros cerebros son los intérpretes de la boleta impresa y nuestras manos asentarán exactamente aquello que hemos contado, sin que medie ningún software.

Es tan fundamental el rol del papel en los comicios que uno de los argumentos de la empresa Magic Software Argentina (MSA) para defender su cuarto oscuro digital y la boleta única electrónica (BUE) es que de todos modos se seguirán manteniendo el impreso y la urna. ¿Entonces estamos invirtiendo dinero exactamente en qué? ¿En relevar a las autoridades de mesa de un trabajo arduo? La democracia es un trabajo arduo. ¿En hacer el proceso más rápido? Ya es bastante veloz tal como está. ¿En que a la larga es más barato? Creo que la democracia es una de esas cosas con las que no deberíamos regatear (llegado el caso de que realmente sea más barato). ¿En que es más equitativo para los partidos chicos? Cierto, pero esto de ninguna manera implica que la boleta electrónica sea la única manera, ni la mejor, de reducir esa brecha. ¿Acaso es para que el acto de votar sea más expeditivo? Hasta donde recuerdo, la Constitución Nacional establece que "el sufragio es universal, igual, secreto y obligatorio", no "práctico y expeditivo".

Con la BUE también se implementan una serie de mecanismos para asegurarse de que lo que está en el chip de la boleta coincide

con el impreso (leer en voz alta antes de pasar el chip), y se imprimen planillas para los fiscales, tal como se explica en el segundo de los comentarios de esta contundente nota de Delia Ferreira Rubio, firmado por el profesor de ingeniería en sistemas Daniel Alonso. Además, sí se pueden enmendar los errores, al revés de lo que se suele decir.

Todo esto está muy bien, pero no cambia el hecho de que se han interpuesto entre el ciudadano y su elección sistemas que el ciudadano no puede fiscalizar por sus propios medios, como se verá enseguida. Por otro lado, si, como ejercicio lógico, pongo en duda la transparencia de las computadoras, ¿por qué debería confiar en que lo que se asienta en las planillas es lo que se termina contabilizando? Hay un punto en el que, por más esfuerzo que se ponga, los comicios electrónicos terminan siendo máquinas hablando con máquinas. Esta es una de las cuestiones que más me preocupan.

Además, si hay fraude usando papel y no pasa nada, el problema no es el fraude, sino el que no pase nada. Dudo mucho que el voto electrónico vaya a resolver esta patología.

Oscuro y digital

Otro de los argumentos que se usaron para fundamentar la validez del sistema que se estrenó en la ciudad de Buenos Aires el último domingo (y en Salta, antes) es que la estación en la que el ciudadano vota no almacena nada, sólo imprime los datos en la boleta y los transmite al chip embebido. No parece una mala idea, pero, lamentablemente, no se puede imprimir nada en este mundo sin que haya software de por medio. Toda impresora es también una computadora, en este caso incorporada a la estación en la que se vota.

En todo caso, si realmente la máquina no almacena nada, ¿dónde se guardarán los registros de seguridad que podrían dar testimonio de que alguien intentó vulnerar el sistema? Estos logs, como se los llama técnicamente, son básicos en la seguridad informática.

Pero hay algo más. Cuando se elige una boleta de papel en el cuarto oscuro y se la deposita ensobrada en la urna, las posibilidades de revelar el secreto del voto son prácticamente nulas. Cualquiera que haya sido autoridad de mesa sabe que eso de que las boletas caen en el orden en que se las depositó y, por lo tanto, se podría establecer quién votó a quién es delirante.

Primero, porque la urna se agita varias veces durante la jornada, para que se asienten los sobres.

Segundo, porque al vaciar la urna el orden de llegada se pierde por completo al derramar el contenido sobre la mesa de recuento.

Tercero, porque, aun si todo esto no fuera así, habría que cotejar el contenido de cada sobre con el acta de los comicios y redactar una lista minuciosa de 200 o 300 nombres y sus respectivos votos -algo groseramente irregular-, y hacerlo delante de los fiscales de varios partidos.

Espiar los comicios electrónicos no es tampoco algo sencillo. El problema no está en la facilidad del fisgoneo, sino, de nuevo, en que podría resultar imposible detectarlo. En este caso, serían máquinas espiando a máquinas.

No digo que vaya a ocurrir. Pero podría hacerse y sin dejar huella, y esto es, por lo tanto, un retroceso. En manos de un gobierno autoritario, la sola posibilidad de un espionaje subrepticio alcanzaría para desalentar el disenso.

Auditoría

Como todo informático sabe que el software tiene vulnerabilidades y puede esconder métodos de espionaje, la frase "código fuente abierto" se menciona siempre como garantía del voto informático y el cuarto oscuro digital. Pero hay un problema también en este aspecto. Como correctamente observó Richard Stallman, sería imposible auditar el código que realmente se ha instalado en cada máquina de votar. No sólo por la enormidad del costo, sino porque habría que fiscalizar incluso el procedimiento de compilar e instalar ese código en cada máquina.

La solución que se implementó en los cuartos oscuros digitales que se usaron en la ciudad de Buenos Aires es arrancar la máquina desde un CD que se saca de un sobre lacrado. Es tecnología del siglo XI y quizá por eso nos suena segura. Es precisamente al revés.

Si existiera una conspiración para reemplazar los discos auditados por otros infectados, el operador, confiado del sello de lacre, no advertiría la diferencia; todos los CD son iguales. Por eso, sería más seguro, aunque ciertamente menos teatral, si en lugar de lacre se usara software firmado digitalmente y estaciones de voto que se negaran a arrancar con CD que no estuvieran firmados.

Le pregunté a MSA si los CD están firmados digitalmente, y me respondieron que no. En cambio, han corrido, me explicaron, una función hash sobre todo el contenido del CD. Es decir que las autoridades de mesa deberían chequear los hashes antes de iniciar los comicios, lo que requiere, desde luego, ejecutar un programa y disponer de cierto conocimiento de informática. "Lo más lógico -me confirmó Hugo Scolnik, fundador del Departamento de Informática de la Facultad de Ciencias Exactas de la Universidad de Buenos Aires y experto en criptografía- sería firmar

digitalmente esos discos. En mi experiencia, nadie se ocupa de cotejar los hashes".

No se entiende

Ahora, ¿todo esto suena muy técnico, no? Ése es justamente el problema. Alemania estableció que el voto informático es inconstitucional porque el ciudadano promedio no entiende nada de estas cosas, ni las va a entender a menos que estudie ingeniería en sistemas. Por lo tanto, no está en condiciones de fiscalizar el acto comicial por sus propios medios. Es mi principal objeción al voto electrónico, el cuarto oscuro digital y la BUE. Aunque fueran infalibles o, al menos, ofrecieran un margen de error mucho menor que el tradicional, no cumplen con un precepto fundamental de la democracia.

El argumento de que el voto digital está más adecuado a las nuevas generaciones no sólo suena un poco discriminatorio (el sufragio debe ser igual), sino que es mayormente falso. Los más jóvenes usan sus equipos sin saber nada de arquitectura de microprocesadores, lenguajes de alto nivel, interpretación, compilación, sistemas operativos, funciones, estructuras de control, protocolos de telecomunicaciones, algoritmos de cifrado y unas cuantas cosas más. Saber que una aspirina te va a calmar el dolor de cabeza no te convierte en médico. Es lo mismo.

Viceversa, todos los ciudadanos entienden bien lo que es elegir una boleta de papel (que permanecerá inmutable), ponerla en un sobre cerrado (que no se abrirá espontáneamente ni revelará más tarde quién lo colocó en la urna) y depositarlo en una caja de cartón (cuyo contenido sólo pueden tocar durante el recuento, por ley, las autoridades de mesa).

De este lado

Aguardé para publicar esta columna porque quería pasar por la experiencia de usar la máquina de votar (la definitiva, no la preliminar que probé en las PASO) y ser testigo de la percepción que los ciudadanos tenían del cambio. Como predije, de lo que menos había que preocuparse era que las personas mayores no entendieran cómo usar el equipo. Hubo algo, en cambio, que me afectó profundamente.

Para evitar caer en el error más torpe de la seguridad informática (dejar solo a un potencial atacante con acceso físico al hardware) se eliminó por completo el cuarto oscuro. Votamos delante de las autoridades de mesa, los fiscales y los ciudadanos que, intrigados frente a la nueva modalidad, estiraban el cuello para ver de qué se trataba. Ese minuto de reflexión a solas sobre el destino de la patria que siempre tuvimos antes de emitir el voto nos fue arrebatado sin más. La exposición pública de ese momento de decisión podría, dicho sea de paso, permitir formas de coerción que ya han sido eliminadas hace décadas.

Oí a muchas personas ponderar lo "rápido y práctico" del sistema. Lo que me llevó a preguntarme qué hemos hecho mal para haber transformado la orgullosa participación democrática en algo tan carente de sentido que queremos despacharlo. Como si fuera un trámite. Creo que debemos reflexionar sobre esto, en especial la clase política.

Quizás en otra década

Como saben los que me leen desde hace algún tiempo, creo en el valor democratizador de las nuevas tecnologías. Creo que facilitan el acceso a la información y a la educación. Creo que el mundo es mejor con computadoras e Internet, del mismo modo que fue mejor con los libros y las ciencias que derivaron de ellos. Incluso creo que nos ayudan a estar menos solos y que hacen las separaciones

menos difíciles de sobrellevar. Pero creo asimismo que hay cuestiones que las máquinas aun no pueden administrar sin intervención humana. El sufragio es una de ellas, en mi opinión. Me siento mucho más tranquilo, pese a ser un promotor infatigable de las nuevas tecnologías, si el primer paso de los comicios no lo dan máquinas hablando con máquinas, sino de personas entregando a otras personas su voto en papel.

Hace varios meses, cuando empecé a trabajar en esta columna, le pregunté su opinión sobre el voto electrónico a Brian Krebs, ex periodista de The New York Times y, hoy, uno de los principales expertos en ciberseguridad del mundo. Me dijo: "La mayoría de los que proponen el voto electrónico reclaman: 'Prueben que es inseguro'. Y los que se oponen replican: 'Prueben que no lo es'. Para bien o para mal, tiendo a alinearme con estos últimos, porque, francamente, la democracia no es algo que uno quiera delegar a unas líneas de código".

También lo consulté a Scolnik, que me respondió: "El voto electrónico se puede implementar en forma inviolable. Pero es imprescindible auditar a fondo los sistemas propuestos. Creo que puede ser mucho menos costoso. O sea hacer un sistema, auditarlo en forma multipartidaria y ponerlo en marcha permitiría hacer el escrutinio muy rápidamente y conservar todos los datos firmados digitalmente por las autoridades de mesa. Pero como no vivimos en un país transparente, mejor dejar las cosas como están. Para hacerlo bien habría que implementar un sistema de auditoría y controles que daría lugar a muchas suspicacias".

Mi opinión está a medio camino entre la de Krebs y la de Scolnik. Tengo la impresión de que el voto informático es lo que eventualmente vamos a terminar usando, porque es una tendencia universal. Todo va migrando lentamente hacia los bits. Pero todavía no tenemos la tecnología para enfrentar una misión tan

crítica como la de los comicios. Faltan quizá décadas para desarrollar algo así. Y cuando lo hagamos -como bien observó Jorge Lanata, uno de los pocos periodistas que trataron estos temas de manera sostenida, informada y responsable- tendremos que debatirlo públicamente. E incluso en ese caso quedará pendiente la cuestión de que, aún con sistemas informáticos invulnerables e infalibles, las máquinas hablan en un idioma que los humanos, incluso los más preparados, no son capaces de comprender.

En esta nota:

- LA NACION
- Tecnología
- Tecnología