EDITORIAL ASTREA

*Reflexiones acerca del voto electrónico**

Por Antonio Aramouni

1. Introducción

A propósito del actual período preelectoral, se ha reinstalado en la Argentina el tema del "voto electrónico", cuyo impulso entre funcionarios y políticos locales se debe a que esa metodología fue utilizada hace poco en Brasil. El rápido escrutinio de las elecciones en las que triunfó Luiz Inácio Lula da Silva, sin que se registraran estridentes reclamos ni impugnaciones, estaría animando la inclinación por tal sistema informático.

Ahora cabe una reflexión: el contexto político argentino difiere del brasileño. Mientras que en el país vecino desde las primeras encuestas hubo ventajas rotundas a favor del candidato que finalmente ganó, en el nuestro varios aspirantes tienen porcentajes cercanos entre sí, con leves variaciones semanales. Nadie se aventura a pronosticar el ganador, sea en la primera vuelta o en el *ballottage*. El caso argentino, en nuestra opinión, puede estimular intentos de violación del sistema computadorizado, si se lo aplicara omitiendo los múltiples recaudos necesarios.

¿Quiénes tendrían interés en perpetrar violaciones del sistema informático con el propósito de manipular los resultados? Por empezar, los contendientes, oficialistas y opositores, ya sea con el guiño o con el *laissez-faire* de las dirigencias partidarias, y también entes o grupos locales y del exterior, tanto de los sectores públicos como de los privados, sin descartar a "francotiradores" que cultiven el resentimiento o el sabotaje. Es que en unas elecciones críticas, realizadas en un contexto harto crítico, en el que estará en juego quién gobernará el ciclo crítico de una transición inocultablemente crítica, hay muchos intereses particulares en juego, divorciados de los intereses del bien público.

2. El fraude informático

No rasgarse las vestiduras ni darse por ofendidos. La violación cotidiana, sistemática, de los más "protegidos" sistemas informáticos del orbe (la Casa Blanca, el Pentágono, la CIA, el FBI, Microsoft, la Bolsa de Valores de Nueva York y tantos otros) muestran las vulnerabilidades que tiene la informática. La piratería informática no respeta ni teme a las víctimas, ni es dominio exclusivo de particulares justicieros, bromistas o vándalos. También hay gobiernos involucrados. Si esto ocurre en ámbitos que cultivan convencidamente la conciencia de la seguridad, imaginemos qué puede suceder, y sucede, en entornos menos cuidadosos.

Es que la seguridad absoluta es una misión imposible, al menos en el orden terrenal. Los millones de instrucciones que contiene un programa (*software*), instrucciones elaboradas entre distintos equipos de numerosos programadores, hace muy difí-

* Extraído del artículo publicado en el diario "La Nación", 14/1/03, p. 15.

cil, humanamente hablando, lograr la perfección total y definitiva de la programación, alma del sistema.

El descuido, torpeza o grieta, en cualquiera de la docena de vías de acceso a un sistema integrado, supuestamente controladas al máximo, será la ocasión, el pase libre, para que ingrese una acción maligna. Así como el actual y tradicional sistema de votación posibilita intentos de fraude (recientes elecciones internas de la UCR y tantos otros sucesos análogos), la propuesta informática adolece de similar debilidad.

Disponer la enorme y compleja infraestructura de *hardware* y telecomunicaciones (servidores de redes locales, regionales y centrales, nodos concentradores, *firewalls* de varios niveles, criptografía muy robusta, sensores automáticos, los más de mil controles cruzados redundantes en tiempo real para cumplir las normas internacionales de calidad ISO 17799/IRAM, demás dispositivos protectores de última tecnología y de *backup*, periféricos y más de 60.000 "urnas electrónicas" conectadas) que requiere la votación *on line* de los 25 millones de empadronados del país, más el sistema automatizado de autenticación del sufragante, más la elaboración de un *software* electoral a prueba de errores y violaciones utilizable en todo el país, que a la vez contemple las particularidades políticas de cada distrito, las previsiones para el procesamiento de la consabida avalancha de votantes en cortos momentos pico, más la puesta a punto mediante testeos y simulacros de tropiezos accidentales o intencionales y de otras contingencias adversas que incluyan el colapso, más garantizar la absoluta transparencia de todos los procesos, es una tarea ingente.

3. Auditoría y seguridad

La capacitación de los miles de asistentes que vigilarán y atenderán inconvenientes y pedidos de ayuda operativa en las mesas de las urnas, más los inevitables reclamos propios de un debut que deban derivarse a las respectivas autoridades electorales, es un detalle adicional por considerar. Si tan sólo el medio por ciento del padrón de 25 millones tuviera problemas, habría 125.000 casos por resolver dentro del horario de la votación.

Pueden hacerse ataques no visibles que dirijan intencionalmente los votos al servidor "equivocado", controlado éste subrepticiamente por adversarios. El votante no está en condiciones de verificar que su voto se corresponde con el que quedó registrado, transmitido o tabulado. No es difícil para un programador escribir un código que muestre en la pantalla el voto real pero registre internamente otro distinto y concluya imprimiendo un resultado premeditado. No tienen manera el ciudadano, las autoridades de mesa ni los fiscales partidarios, de asegurarse de que eso no ocurra dentro de la "caja negra".

Los protocolos del *software* para votar electrónicamente, además de proteger la privacidad, deben autenticar al elector, asegurando que sólo los ciudadanos habilitados (ni los muertos ni los impedidos jurídicamente) puedan votar, que nadie pueda votar más de una vez, que nadie pueda robar identidad ajena, que nadie pueda conocer por quién se ha votado, que nadie pueda votar por otro, que nadie pueda cambiar el voto ajeno y que cada votante pueda confiar en que su voto esté incluido correctamente en el escrutinio. La depuración comprobada de los padrones, requisito lógico

para la inauguración prolija del emprendimiento que nos ocupa, es un trabajo clave aún pendiente.

Se impone implementar la especializada auditoría y seguridad de sistemas de informática, desde los programas fuente hasta cada componente funcional, volcándole toda la "enciclopedia" teórico-práctica y el arsenal de instrumentos y medios de esta disciplina, con la calificación aprobatoria emanada de un comité pluridisciplinario independiente de reconocidos expertos, rigurosa y debidamente conformado.

4. La pausa judicial

Antes, durante y después del cierre de los comicios se producen muchísimas intercomunicaciones entre los funcionarios y agentes de los diversos organismos involucrados en ellos, así como con las autoridades partidarias y el periodismo, lo cual exige otorgar autenticidad, integridad y disponibilidad inmediata tanto a las fuentes como a los emisores y a los receptores de tales informaciones, por lo que el recomendado mecanismo de "firma digital" será insoslayable.

Concluido el acto, y ya en el tramo del posescrutinio, sobrevendrán previsibles reclamos, acusaciones e impugnaciones, fundados o no, que se dirimirán en la instancia judicial (recordemos el estupor e incluso la sospecha sobre la definición de las elecciones presidenciales estadounidenses ocurrida en el estado de Florida, cuando finalmente el 6 de enero de 2001 George W. Bush fue proclamado vencedor) lo cual exigirá acudir a la informática forense, que investigará los procesos y las telecomunicaciones, los elementos involucrados, las pistas de auditoría electrónicas y complementarias, y la documentación de los controles, atendiendo así a la obtención, exposición y celosa custodia de las pruebas, a la producción de pericias y a confrontarlas con probables contrapericias de oposición, para ser todo elevado al dictamen del juez y quizá después a los niveles de apelación. Entretanto, inferimos, debería aguardarse el veredicto sobre el resultado de las elecciones. Una pausa de incierta duración.

En materia de seguridad nos queda mucho por decir. Nuestra abreviada enunciación intenta brindar sólo una imagen conceptual de los riesgos y previsiones inherentes a una instancia cívica crucial, con influencia decisiva en el destino próximo del país.

Lejos de cuestionar el sistema automatizado, señalamos sus problemas y sus necesarios resguardos. Computadorizar las elecciones aventaja al sistema manual. No sólo economiza tiempo y disgustos sino que ofrece, como subproductos cuasi gratuitos, una serie de "mapas sociopolíticos", estadísticas e índices, que conforman un virtual y utilísimo censo cívico. Una licitación para proveer la informatización eleccionaria, sea o no llave en mano, deberá tener en cuenta el repertorio de los requisitos expresados y someterse a la auditoría y pruebas de calidad por parte del ente independiente de expertos al que hicimos referencia.

Considerando el escenario descripto, decidir hoy la adopción apresurada, incondicional, del voto electrónico para las anunciadas elecciones de abril es una ilusión prematura: sería pura gula informática. La gula empacha. Y no nutre.