El Rol de las Cuatro Libertades Esenciales en los Sistemas de Voto Electrónico Directo

Marcela Capobianco Alejandro G. Stankevicius

Laboratorio de Investigación en Sistemas Distribuidos
Departamento de Cs. e Ing. de la Computación
Universidad Nacional del Sur
Bahía Blanca - Buenos Aires - ARGENTINA
e-mail: {mc, ags}@cs.uns.edu.ar

Resumen

En la actualidad se puede reconocer una fuerte tendencia a propugnar la adopción de sistemas de voto electrónico en las distintas compulsas electorales. La piedra basal de este tipo de sistema es el software que corre en cada puesto de votación, debiéndose tener gran cuidado de no claudicar derecho alguno de los votantes al llevar adelante la instauración del nuevo sistema. Este artículo analiza en particular el rol que pueden desempeñar las cuatro libertades esenciales del software libre en relación al software de los sistemas de voto electrónico directo.

Del estudio reportado se arriba a una importante conclusión: estas cuatro libertades constituyen un requisito necesario pero al mismo tiempo insuficiente, ya que meramente hacer uso de software libre no alcanza para preservar la totalidad de los derechos de electores, puesto que las mismas técnicas empleadas para atacar sistemas de software en general pueden ser usadas para vulnerar este tipo de sistemas.

Palabras Clave: software libre, voto electrónico, seguridad en sistemas, firma digital

1. Introducción

Incidentalmente el año en curso es lo que se denomina en la jerga un "año electoral", producto de las distintas convocatorias a elección que se han de suceder a lo largo del año, concluyendo con la elección a presidente del mes de octubre. Los años electorales se caracterizan por una alta presencia en los medios de los candidatos de las distintas agrupaciones políticas. A su vez, también se caracterizan por el resurgimiento de una crítica un tanto artera hacia el actual sistema de elección, especialmente toda vez que se produce alguna irregularidad como fue el caso recientemente en la elección a gobernador de la provincia de Santa Cruz. Aparentemente, según se desprende de las manifestaciones de distintos políticos y politólogos, existe una alternativa superadora a la espera de ser adoptada la cual nos evitaría este tipo de inconvenientes: el *voto electrónico*. Este concepto engloba muy diversas tecnologías. La literatura [17] clasifica a los distintos sistemas de voto electrónico en tres categorías bien diferenciadas, a saber:

1. Los *sistemas de recuento electrónico de votos*.
2. Los *sistemas de voto electrónico directo* (o DRE, según su sigla en inglés).
3. Los *sistemas de votación a distancia* a través de internet.

Los sistemas de recuento electrónico de votos apuntan principalmente a automatizar el componente quizás más tedioso y por ende principal fuente de errores del sistemas tradicional: el escrutinio. La idea es hacer uso de reconocedores ópticos para detectar las marcas o perforaciones hechas en las boletas por los electores simplificando de esta forma el tabulado de los votos. Por otra parte, los sistemas de voto electrónico directo tienen por objeto sistematizar la totalidad del acto eleccionario, informatizando los padrones, el acto mismo de la emisión del sufragio y también el posterior escrutinio. Algunos sistemas incluso se encuentran en red por lo que al mismo tiempo que se cierra una urna se puede estar tabulando el resultado general de la elección (es decir, se automatiza incluso lo que en el sistema tradicional corresponde al envío del telegrama con los resultados por parte del presidente de mesa). Finalmente, los sistemas de votación a distancia atacan un problema diferente si bien también asociado a la realización del

acto eleccionario: el inconveniente que presente el no estar físicamente en cercanías a la urna en la cual el padrón electoral dictamina debemos emitir nuestro sufragio. El sistema actual contempla la excepción a la emisión del voto (que recordemos en nuestro país es obligatorio) cuando el elector se encuentra por caso a más de 500kms de su domicilio, o bien convaleciente y por ende imposibilitado de acercarse a la correspondiente mesa.

Mucho se ha dicho de las tan mentadas virtudes de estos tres tipos de sistemas. Naturalmente la mayor parte de los argumentos a favor fue vertida por quienes se verían beneficiados con la adopción de estos sistemas, por caso, los proveedores del hardware, los desarrolladores del software, etc. En contraste, no tanto ha sido dicho ni publicado respecto de los inconvenientes y hasta papelones o incluso fraudes a escala masiva que se detectaron en más de una ocasión no sólo en Argentina sino en el mundo [8, 2, 6]. Seguramente el caso más conocido sigue siendo la elección a presidente en Estados Unidos en el año 2000, donde tuvo que intervenir la corte suprema para restaurar la legitimidad perdida por el flagrante fraude en la designación de los electores que correspondían al estado de Florida. El tipo de boleta perforada que se utilizó en dicha elección imposibilitó que el órgano que equivale a nuestra Junta Electoral pueda verificar los resultados reportados por los presidentes de mesa, ya que la mera manipulación de las tarjetas de voto adulteraba la intención del elector (el troquelado de muchas de las tarjetas se desprendía al más mínimo contacto, registrando en ocasiones más de un votos para la misma categoría, tornando por ende inválido un voto inicialmente ajustado a derecho).

De los tres sistemas de voto electrónico reseñados, el presente artículo se focaliza exclusivamente en el segundo tipo, esto es, en los sistemas de voto electrónico directo. La piedra basal de este tipo de sistema es el software que ha de correr en cada puesto de votación, debiéndose tener gran cuidado de no claudicar derecho alguno de los votantes al llevar adelante la instauración del sistema. Ejemplo de esto último abunda en la literatura técnica, por caso el trabajo de Feldman y otros [3] resume cómo a través de medios a disposición de cualquier interesado es posible adulterar la voluntad de los electores en caso de hacer uso del sistema AccuVote-TS de la compañía Diebold. Evidentemente se debe tener bastante cuidado al especificar las características que el software que va a correr en los puesto de votación de un sistema de voto

electrónico directo ha de cumplir.

Recordemos que el software es usualmente creado por uno o varios programadores quienes reservan para sí o para la empresa en donde trabajen la totalidad de los derechos acerca de esa creación. Asociado a toda pieza de software suele venir una *licencia de software*, el mecanismo usualmente adoptado para permitir que un tercero (el usuario) tenga derecho a hacer uso de un determinado programa. La licencia de software es en esencia un contrato entre el dueño del programa y los usuarios, en donde se suele indicar con bastante precisión qué se puede y principalmente qué no se puede hacer con el programa. Esta es la situación en general con el software tradicional, pero también existe otra vertiente, en donde el software en vez de privar de derechos a sus usuarios opta por garantizarles ciertas libertades. A este tipo de software se lo denomina *libre* y por contraposición al software tradicional se lo denomina *privativo*.

La formalización del concepto de software libre viene de la mano del proyecto **GNU**, inicialmente una cruzada personal del Richard M. Stallman cuyo propósito consistía en crear un sistema operativo completamente libre [12]. En este sentido, el software libre se centra en asegurar que los usuarios sean capaces de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Para esto, una pieza de software se denomina libre sí, y sólo sí, asegura las siguientes cuatro libertades esenciales:

Libertad 0 La libertad de ejecutar el programa, para cualquier propósito.

Libertad 1 La libertad de estudiar cómo trabaja el programa, y cambiarlo para que haga lo que el usuario quiera. Tener acceso al código fuente es una condición necesaria para esto.

Libertad 2 La libertad de redistribuir copias para colaborar con el resto de la sociedad.

Libertad 3 La libertad de distribuir copias a terceros de las versiones modificadas por el usuario. De optar por hacerlo, el resto de la sociedad está en condiciones de beneficiarse de esos cambios. Una vez más, tener acceso al código fuente es una condición necesaria también para esto.

En otras palabras, se puede afirmar que un programa constituye software libre si sus usuarios gozan de de la totalidad de estas libertades. Es decir, todo usuario debería ser libre de

redistribuir copias, ya sea con o sin modificaciones, libre de costo o bien recibiendo una contrapartida por la distribución, sin limitación alguna de a quién ni en dónde llevar adelante esa distribución. Estas libertades, al estar aseguradas por el software libre implican que el usuario no necesita pedir permiso ni negociar una licencia especial con los autores para emprender estas actividades. Estas sencillas cuatro libertades están revolucionando no sólo la formal en que los usuarios usan las computadora y los programas sino también la manera en qué esos programas se desarrollan, se mantienen actualizados, se depuran de los errores que se detecten e incluso la forma misma en que se conducen negocios en la industria del software.

En este sentido, el reputado hacker Eric S. Raymond fue uno de los primero en reconocer que el modelo de desarrollo de software libre, el cual involucra usualmente gran cantidad de desarrolladores y por qué no hasta los propios usuarios finales, redunda en un software de mejor calidad bajo las métricas usuales (por caso, nivel de documentación del código fuente, tiempo promedio entre la detección y la corrección de un error, etc.). El análisis detallado del proceso mental que le permitió arribar a esta no tan evidente conclusión está cuidadosamente recopilado en el trabajo seminal "La Catedral y el Bazar" [9].

Entre los distintos aspectos que resulta atractivo estudiar y considerar en detalle de los sistemas de voto electrónico directo, el presente artículo se circunscribe a explorar y determinar el impacto que conllevan las cuatro libertades esenciales del software libre en el marco de este tipo de sistemas. A tal efecto la siguiente sección repasa las principales características de los sistemas de voto electrónico directo, bosquejando su organización e identificando tanto virtudes como potenciales desventajas. Luego, la sección 3 desarrolla el análsis del impacto que tienen las cuatro libertades esenciales, a fin de determinar si el hacer uso de software libre es una condición suficiente y necesaria para atender los cuestionamientos identificados en la sección 2. Finalmente, la sección 4 sintetiza las principales conclusiones obtenidas a lo largo del desarrollo del trabajo.

2. Los Sistemas de Voto Electrónico Directo

Esta sección tiene por objeto repasar la organización y principales características de los sistemas de voto electrónico directo, identificando a la par cuáles son las virtudes y los aspectos cuestionables que presentan este tipo de sistemas. Para esto, la sección 2.1 analiza la organización tradicional que suelen adoptar los sistemas de voto electrónico directo, enumerando el rol de sus distintos componentes. Luego, la sección 2.2 sintetiza brevemente los principales beneficios que aportan este tipo de sistema. Finalmente la sección 2.3 hace lo propio con los potenciales riesgos implicados en la adopción de este tipo de sistemas.

2.1. Organización

La organización de un sistema de voto electrónico directo en concreto depende naturalmente de la organización del sistema de voto convencional al cual está supeditando. A manera de simplificación, asumiremos una organización para el sistema de voto convencional en proceso de ser informatizado análogo al utilizado en nuestro país. En otras palabras, asumiremos que la elección se lleva adelante en distintos centros de votación, en los cuales han de existir una determinada cantidad de mesas de votación (que mantienen el anacronismo de distinguir por sexo), donde cada mesa de votación tiene asociado una urna, un padrón que identifica unívocamente a conjunto de votantes, un cuarto oscuro para preservar carácter secreto del sufragio, así como un conjunto de autoridades las cuales tienen la responsabilidad de preservar los derechos de los electores consagrados en el Código Electoral Nacional (Ley 19.445).

Siguiendo esta organización, los sistemas de voto electrónico directo cuentan con los siguientes componentes:

- Una base de datos general en donde se tabulan los resultados globales de la elección.
- Una base de datos local a cada centro de votación en donde se recopilan los resultados parciales de las mesas de ese centro de votación.
- Uno o más dispositivos para registrar la participación de los votantes en el acto eleccionario.

- Un dispositivo a ser instalado en cada cuarto oscuro el cual será usado por los electores para emitir los votos.

Como puede apreciarse, el correlato con los componentes del sistema de votación actualmente en uso es inmediato: la base de datos general reemplaza al centro de cómputos, la local a la planilla totalizadora de los fiscales generales de las agrupaciones políticas, el dispositivo para registrar la participación de los votantes supedita a los vetustos padrones impresos en papel y por último, el dispositivo usado para emitir los votos reemplaza a la urna, las boletas, los sobres e incluso a la planilla para tabular el escrutinio.

El rol de la base de datos general es ir concentrando los resultados parciales producidos por las distintas bases de datos locales, mientras que el rol de estas últimas es hacer lo propio con los resultados que vayan surgiendo de los distintos puestos de votación. Los puestos de votación pueden o no estar en red con la base de datos local; de la misma forma, la base de datos local puede o no estar en red con la base de datos general. Naturalmente, resulta más conveniente contar con una conexión de red, pero el costo de la instauración de tal infraestructura para ser usada sólo en el acto eleccionario puede superar ampliamente a los beneficios que aporta.

En relación al dispositivo para registrar la participación de los votantes en el acto eleccionario, se han ensayado diversas alternativas, desde hacer uso de una computadora convencional tipo netbook o tableta hasta dispositivos de propósito específico construidos a tal efecto. De igual forma, el dispositivo utilizado por los electores para emitir sus votos ha asumido las más diversas configuraciones. Sin desmedro de los restantes componentes, este último es sin duda el más trascendente pues constituye el artefacto con el cual interactuarán obligatoriamente los votantes. En general, en estos dispositivos se pueden identificar los siguientes componentes internos de hardware:

- Un dispositivo de salida en el cual presentar la interfaz del sistema.
- Opcionalmente un dispositivo de salida secundario para ir generando un correlato físico de las boletas virtuales que vayan creando electores al sufragar.
- Un dispositivo de entrada a través del cual los usuarios han de interactuar con el sistema.

- Un procesador central encargado de ejecutar al software que controla el dispositivo.
- Una jerarquía de almacenamiento en donde llevar registro del estado de la ejecución del programa.

El dispositivo de salida es usualmente una pantalla. En algunas configuraciones se cuenta con un dispositivo de salida secundario, por caso auriculares, para los electores que tengan alguna dificultad para visualizar lo presentado en la pantalla. De igual forma, alguna configuraciones también cuentan con un impresora usualmente enclaustrada en una urna transparente como para que los votantes puedan tomar contacto con su sufragio. Este es un aspecto un tanto atávico, quizás las nuevas generaciones no tengan tanto inconveniente en lograr relacionarse con la versión virtual del sufragio (esto es, el incremento en uno de un cierto valor almacenado en una determinada posición en la memoria del dispositivo).

Con respecto al dispositivo de entrada, las primeras versiones hacían uso de un pequeño teclado pero las variantes más recientes hacen uso de una pantalla táctil a fin de simplificar la interacción con los electores. En relación al procesador central, existen diversas alternativas, desde usar un procesador de propósito general, como el presente en las computadoras de escritorio, hasta hacer uso de uno de propósito específico, como el incluido en celulares y smartphones. La elección que se haga afectará principalmente al conjunto de herramientas a disposición de los desarrolladores del software del sistema, si bien no tanto a los usuarios finales, quienes difícilmente estén en condiciones de aventurar qué arquitectura subyace a la interfaz con la cual interactúan.

Finalmente, el uso que se le da a la jerarquía de memoria excede el rol usual que se la da a los distintos niveles de almacenamiento (esto es, memoria cache, memoria principal, memoria secundaria, etc.), ya que parte de los datos almacenados en la jerarquía han de representar los sufragios de los electores, los cuales deben ser manipulados con extrema precaución. En algunos casos se hace uso de un dispositivo de almacenamiento removible el cual es usado para transferir los resultados de una determinada mesa a la base de datos local del centro de votación. En otros casos se utiliza algún almacenamiento de tipo WORM (Write Once Read Many) para ir dejando constancia de la operatoria del dispositivo a lo largo de la jornada de votación.

En síntesis, es evidente que los componentes internos de hardware del dispositivo para emitir los votos describen en esencia a una computadora convencional, razón por la cual las primeras implementaciones hacían uso directamente de computadoras de escritorio. Este modelo fue posteriormente abandonado por los riesgos que implica llevar adelante una tarea tan sensitiva en una plataforma la cual puede resultarle familiar a los eventuales interesados en adulterar el resultado de la votación.

Considerado en detalle el hardware disponible, sólo resta elaborar acerca del software. En este sentido, en general existen básicamente dos piezas de software corriendo en sobre este hardware, a saber:

- El programa propiamente dicho, el cual implementa el sistema de voto de voto electrónico directo.
- Opcionalmente un sistema operativo capaz de administrar los dispositivos de entrada y de salida con los que cuente el dispositivo.

En función de las decisiones de diseño tomadas a la hora de implementar el sistema de voto electrónico directo existen dos alternativas: que el propio programa asuma las funciones del sistema operativo [14], o bien que el programa sea más convencional y haga uso de los servicios de un sistema operativo aparte. Las ventajas y desventajas de las distintas decisiones de diseño antes reseñadas serán analizadas las secciones 2.2 y 2.3.

2.2. Principales Beneficios

Cabe reiterar que mucho se ha dicho y mucho ha sido publicado acerca de los fantásticos beneficios de este tipo de sistemas. A continuación intentaremos resumir los argumentos más sólidos propuestos en las publicidades y propagandas de los propios fabricantes, identificando las virtudes provistos por la automatización del proceso electoral.

En primer lugar, la informatización del centro de cómputos general es algo con lo que contamos hoy en día. Al mismo tiempo que se van recibiendo los telegramas totalizando el escrutinio

una determinada mesa, éstos son volcados en un sistema informático que va tabulando y calculando los porcentajes de votos obtenidos por los distintos candidatos. Incluso recientemente se incorporó la posibilidad de ser testigo en vivo de este proceso de carga a través de la página web del Ministerio del Interior, característica que hace aún más transparente al acto eleccionario.

En relación a la base de datos local a cada centro de votación, en la actualidad no existe un sistemas informático que simplifique la tarea de recopilar los resultados de las distintas mesas. Para muestra basta ver lo que sucede en los centros de votación cuando llega la hora del cierre, los fiscales generales entran en un frenesí, y calculadora en mano intentan proyectar qué tal les fue en la elección. La combinación de este sistema local con el general permitiría eliminar una fuente de fraude varias veces empleada que gira en torno a la custodia de la urnas conteniendo los votos una vez finalizada la elección. El dispositivo de seguridad que se debe montar luego de cada elección es escalofriante, no sólo en magnitud sino también en importancia. Esas débiles urnas de cartón reflejan la voluntad de cientos de ciudadanos, por lo que deben ser custodiadas como si estuvieran construidas en oro puro. Todo este andamiaje puede o podría ser eliminado o al menos reducido sensiblemente en su tamaño simplemente digitalizando el contenido de las urnas. La clave está en que es trivial crear un duplicado exacto de cualquier documento digital, mientras que no es tan sencillo duplicar una urna y su contenido. Este concepto encaja a la perfección con la informatización de la emisión del voto, pues de esta forma el voto no requiere ser digitalizado a posteriori, sino que existe de manera digital desde el momento de su creación.

Otro aspecto en donde los beneficios superan ampliamente a los riesgos es en la informatización del padrón electoral. Si bien es cierto que en las mesas se suele adoptar una suerte de esquema en paralelo, donde mientras un elector entra al cuarto oscuro, al siguiente le están verificando el documento y lo están consignando en el padrón, de todas formas las búsquedas a mano en el padrón resultan tediosas y por ende propensas al error. La mera automatización de esta tarea, realizando la búsqueda directamente por número de DNI, permitiría que las autoridades de mesa dediquen su atención a controlar otros aspectos más relevantes (por caso, que el elector presente el documento que figura en el padrón, etc.).

Finalmente corresponde considerar los beneficios de hacer uso del dispositivo que automati-

za la emisión del voto. En principio el considerable esfuerzo de modificar el sistema de votación convencional tiene por objeto permitir hacer uso de estos dispositivos puesto que se postula proveen gran cantidad de beneficios. Por caso, los fabricantes de estos sistemas sostienen que las pruebas a pequeña escala realizadas muestran que se reduce el tiempo promedio dentro del cuarto oscuro. Otro beneficio tangible es que de contar con dispositivos de salida alternativos como auriculares es posible simplificar la estadía en el cuarto oscuro de aquellos votantes con dificultades en la vista. El actual código electoral contempla que el presidente de mesa es el encargado de asistir a este tipo de votantes, lo cual impone una responsabilidad adicional al ya bastante atiborrado presidente. Un beneficio más sutil es que el sistema de voto electrónico directo puede proveer retroalimentación al votantes ayudándole a evitar que invalide accidentalmente su voto. Recordemos que en el sistema actual es muy fácil cometer un descuido que invalide nuestro voto al introducir las boletas en el sobre, especialmente si se apeló al corte de boleta. En este sentido, tampoco se corre riesgo de que se agoten las boletas de un dado partido, o que algún fiscal inescrupuloso se dedique a destruir las boletas de la competencia. Este aspecto resulta especialmente provechoso para los partidos políticos chicos, los cuales están obligados por ley a hacer frente al costo de impresión de las boletas, debiendo cubrir un número en ocasiones bastante mayor que la cantidad de votos que eventualmente han de recibir.

Una vez finalizado el acto eleccionario llega el momento quizás más engorroso, el escrutinio primario que se desarrolla en el mismo cuarto oscuro. La apertura de los sobres, la determinación del estado de cada uno de los votos (ya sea válido, en blanco, anulado, impugnado, etc.), el tener que lidiar las boletas parciales producto del corte y finalmente el recuento en sí de los votos son tareas que más de una autoridad preferiría evitar luego de haber estado más de diez horas a cargo de la mesa. Es aquí donde contar con un sistema informático redunda en un máximo beneficio, ya que el escrutinio se vuelve instantáneo, la determinación del estado de los votos resulta inmediata,[1] y por ende la obtención del resultado final pasa a ser algo tan simple como apretar un botón.

[1]incluso es posible implementar que las autoridades de mesa cuenten con la posibilidad de impugnar votos

2.3. Potenciales Riesgos

De lo expuesto en la sección anterior, resulta sorprendente que no se estén usando sistemas de voto electrónico directo para llevar adelante la totalidad de las elecciones del país. Si bien es cierto que el sistema actual cuenta con múltiples puntos flacos (por caso, tener que custodiar las urnas luego del acto eleccionario), el adoptar un nuevo sistema viene necesariamente acompañado de riesgos no contemplados [4, 2]. Es posible que los nuevos riesgos resulten equivalentes a los preexistentes, o que resulten menos preponderantes que los beneficios que se han de capitalizar. De una forma u otra, estos riesgos existen y deben ser cuidadosamente estimados, por lo que dedicaremos el resto de esta sección a intentar identificar los principales inconvenientes que trae aparejado la adopción de un sistema de voto electrónico directo, respetando el mismo orden de presentación que el desarrollado en las secciones anteriores.

En primer lugar, la existencia de una base de datos global puede constituir un punto vulnerable si no se adopta una adecuada política de seguridad, tanto física como lógica, especialmente si no se cuenta con un respaldo físico de los sufragios (en algunas configuraciones se generan un comprobante en papel por cada voto emitido, los cuales pueden ser custodiados de manera análoga a lo que se hace con las urnas en el sistema convencional). Este es un punto crucial si consideramos lo que se encuentra en juego. Por caso, en el sistema convencional el escrutinio en cada mesa no es de última instancia; siempre es posible interponer alguna forma de recurso el cual eventualmente involucra revisar el registro físico de los votos (esto es, abrir de nuevo la urna y recontar los votos). Todo sistema de voto electrónico directo razonable debe hacer uso de la técnica de *firma digital* [10, 11] a fin de garantizar la inalterabilidad de los registros de la base de datos global. Naturalmente, quien tenga acceso a la clave privada utilizada para firmar esos registros estará en condiciones de adulterarlos sin dejar rastro, por lo que mantener una adecuada custodia de estas claves es un aspecto también central. De más está decir que la custodia no puede ser dejada en manos de la compañía proveedora del hardware y el software usado en el acto eleccionario. Estas mismas consideraciones pueden ser argumentadas en el marco de la base de datos local, si bien las consecuencias de una manejo incorrecto de los registros tendrá un impacto evidentemente circunscripto a las mesas de ese centro de votación.

En cuanto al dispositivo para registrar la participación de los votantes, a priori no parece generar riesgo alguno, puesto que a lo sumo si la autoridad de mesa se olvidara de registrar a un votante, el mismo de todas formas cuenta con el comprobante físico de que en efecto votó (léase, el sello en su DNI). No obstante, si consideramos el sistema convencional hay un detalle importante que vincula este registro con la emisión del voto propiamente dicho: el sobre entregado por el presidente de mesa y firmado por las autoridades. Quien no figure en el padrón o quien no esté en condiciones de justificar fehacientemente ser quien dice ser no recibirá uno de esos sobres (o en el mejor de los casos sólo recibirá un sobre especial por tratarse de un voto en proceso de ser impugnado). La razón de ser de este peculiar mecanismo contemplado en el código se origina en el acertado diagnóstico de sus autores de las deleznables prácticas en las que incurren algunos ciudadanos. Por ejemplo, hay quienes intentan direccionar el voto de otras personas suministrando previamente un sobre cerrado para que sea puesto directamente en la urna, o bien cohercionando a los votantes para que marquen su sobre a fin de que se pueda verificar una vez llegado el escrutinio que votaron de la manera que le fuera indicada. Afortunadamente la reglamentación vigente evita este tipo de práctica, suministrando el sobre con determinadas firmas (que no se pueden conseguir antemano) o rechazando los sobres que puedan ser individualizados. En este sentido, es esencial que el sistema de voto electrónico directo cuente con alguna forma de testigo, a ser producido por las autoridades de mesa en el preciso momento en que se presenta el votante, el cual ha de actuar como llave posibilitando a esa persona y no a otra a emitir el sufragio. Los mecanismos contemplados para poder identificar los votos impugnados bien pueden ser incorporados en ese testigo, para luego ser registrados por el dispositivo electrónico de votación.

Por último, el punto más vulnerable y por ende cuestionable de los sistemas de voto electrónico directo es justamente el dispositivo presente en el cuarto oscuro. El análisis de los riesgos aparejados a este apartado ameritan un artículo entero en sí mismo. Por caso la vulnerabilidad de la totalidad del sistema por tratarse de dispositivos electrónicos los cuales requieren un flujo constante de electricidad para su correcto funcionamiento. Este cuestionamiento ha sido soslayado en más de una oportunidad señalando que hoy en día se cuenta con suministros alter-

nativos de electricidad como ser baterías o generadores portátiles. Por razones de espacio nos vemos obligados a concentrar nuestra atención en los riesgos a nivel de software principalmente, teniendo en cuenta que nuestro objetivo final es analizar el impacto de las libertades implicadas por la licencia utilizada.

En este sentido, las primeras intentonas de adopción de sistemas de voto electrónico directo apelaron a la técnica de *seguridad por oscurecimiento* [1], la cual si bien válida en determinados contexto es demostrablemente inapropiada en este tipo de sistemas. Por caso, la compañía Diebold, creadora de múltiples soluciones para voto electrónico, hace uso de una licencia privativa conservando oculto el código fuente de los programas utilizados. Esta decisión dificulta notablemente el accionar de los auditores, ya que para tomar contacto con este código usualmente se ven forzados a suscribir acuerdos de confidencialidad, mancillando su imparcialidad. En una ocasión se difundió accidentalmente una instantánea del código fuente de uno de estos dispositivos de votación, lo que posibilitó que múltiples centros de investigación se dedican a analizar los mecanismos de seguridad incorporados en el programa. Las conclusiones obtenidas en esos trabajos rayan la inverosimilitud; el trabajo de Kohno y otros [6] afirma que se detectaron numeras fallas de seguridad y que el análisis de código fuente no revela que la seguridad haya sido tenida en cuenta como objetivo de diseño.

Otro aspecto no menos relevante es el riesgo asociado a la complejidad inherente a la interacción con todo sistema de software. Concretamente, el problema que se está atacando con este tipo de sistemas no está apuntado a un segmento parcial de la población sino a su totalidad. Se debe contemplar que el sistema debe resultar accesible a todo tipo de ciudadano, con todo tipo de formación. Esto es, ¡el sistema ni siquiera puede asumir que el usuario sabe leer y escribir!

Repasando los componentes internos de hardware del dispositivo de votación se puede apreciar que las unidades que cuenten con un dispositivo de salida secundario en donde ir registrando físicamente los votos efectuados introducen nuevas formas de riesgo como ser que la impresora se quede sin papel o sin tóner. El sistema convencional evita estos riesgos llevando adelante la impresión de las boletas de manera anticipada. Por otra parte, aquellos que cuenten con un dispositivo de entrada estilo teclado son pasibles de sabotaje. Por caso, si se conoce de antemano

en qué ubicación estará un dado candidato al cual se lo desea perjudicar, se puede alterar el contacto de la tecla asociada a esa opción. El mecanismo natural para contrarrestar este ataque es que los candidatos se ordenen al azar cada vez que sean mostrados en pantalla.

Finalmente, el punto más crítico del dispositivo en donde se lleva adelante la votación es el subsistema de memoria, en particular la unidad de almacenamiento en donde se van tabulando los votos. En este caso el riesgo no sólo incluye que sea accedido físicamente (destruyendo su contenido), sino que existen riesgos mucho más imperceptibles. Puntualmente el sistema electoral convencional consagra, entre otras, dos cuestiones esenciales: la integridad y el secreto del voto. Un gran número de las medidas presentes en el Código Electoral Nacional, que a simple vista pueden parecer desproporcionadas, tienen por objeto preservar y defender estas cuestiones precisamente. Al informatizar el sistema se debe tener especial cuidado de claudicar la integridad y el secreto del voto. Pero esta no es una tarea simple. Para asegurar la integridad del voto se debe mantener un registro de cuáles fueron, lo cual fácilmente conduce a perder el secreto. De igual forma, privilegiar el secreto del voto torna bastante más complejo asegurar la integridad del mismo. Este problema no es insoluble, requiere un acertado uso de las técnicas de firma digital y de encriptado [5, 7, 15], lo que nuevamente implica que se deba custodiar con especial cuidado las claves privadas que se estén utilizando.

Otro riesgo no menos significativo hace mella justamente a uno de los aspectos más destacados al analizar los beneficios: la automatización del escrutinio. Bajo el sistema convencional cualquier persona que sepa contar está en condiciones de participar del escrutinio y verificar que los datos consignados en la tabla resumen sean fidedignos. En contraste, al informatizar la elección muy pocas personas estarán en condiciones de llevar adelante tal verificación. El resultado del escrutinio al usar un sistema de voto electrónico directo se asemeja más a las encuestas de boca de urna publicadas a segundos del cierre del comicio, las cuales dictaminan quién se adjudicó la elección. De la misma forma que el público en general no está en condiciones de verificar las conclusiones de ese tipo de encuestas, tampoco estarán en condiciones de verificar los resultados del comicio. A la luz de esto cobra todavía más trascendencia que las auditorias del funcionamiento del sistema sean altamente imparciales.

3. El Rol de las Cuatro Libertades Esenciales

Esta sección elabora sobre la base de los riesgos antes identificados, analizando en particular el rol de las cuatro libertades esenciales del software libre, puesto que es posible que estas libertades permitan contrarrestar o al menos atemperar el impacto de los distintos riesgos. El objetivo último es determinar si contar con estas cuatro libertades constituye un requisito suficiente y necesario a fin de garantizar que no sean vulnerados los derechos de los electores. En este sentido, analizaremos el aporte cada libertad esencial por separado para luego considerar un efecto que se desprende de la segunda y la cuarta: el garantizar el acceso al código fuente del programa.

En primer lugar, la **Libertad 0** trae aparejado una consecuencia beneficiosa para los peculios del estado. Como esta libertad asegura que el software puede ser usado sin tener que tramitar un permiso especial o abonar costo alguno, usar software libre reporta un ahorro económico inmediato. Claro está, este beneficio sólo abarca al software, no así al hardware o al resto de la infraestructura.

Con respecto a la **Libertad 1**, entendemos que constituye un derecho irrenunciable de quien encargue la implementación del un sistema de voto electrónico directo (esto es, el estado). En la sección anterior se mencionó las dificultades que trae aparejado no tener acceso libre al código fuente del software, en particular a la hora de llevar adelante las necesarias auditorias, y que la imparcialidad de éstas resulta fundamental a la hora de restaurar la confianza de los ciudadanos en el resultado de la elección. Recordemos que el poder investido en las autoridades designadas por el voto popular pivota en la legitimidad del acto eleccionario (las recientes elecciones presidenciales en Honduras dan cuenta de ésto).

Las **Libertades 2 y 3**, de gran importancia en la industria del software, parece pasar a un segundo plano al considerar sistemas de voto electrónico directo, ya que versan acerca de la redistribución de copias, ya sea en su versión original o bien habiéndose incorporados modificaciones. No obstante, los terceros interesados en estudiar, alterar y quizás compartir con la sociedad sus modificaciones al sistema, sí se benefician de manera directa de estas libertades. Estamos haciendo referencia típicamente a los centros de investigación (tales como

las organizaciones no gubernamentales o las propias universidades nacionales) que ávidamente toman contacto para analizar y estudiar estos tipos de sistemas, señalando las falencias que se detecten. Estos terceros desempeñaron un rol preponderando en el desenmascaramiento del bochorno de la compañía Diebold [6, 3]. Tan irremontable fue el daño sufrido por el prestigio de esta compañía que decidió "matar" a la marca, pasándose a llamar Premier Election Solutions en agosto de 2007.

Finalmente, de las **Libertades 1 y 3** se desprende que el código fuente del programa tiene que estar a disposición de quien así lo solicite y sin adulterar (esto es, sin ofuscar). Usualmente el disponer del código fuente se considera la panacea universal para todos estos riesgos. Sin embargo, esta tesitura deviene de un entendimiento imperfecto del proceso de obtención del programa que finalmente ejecuta en el procesador a partir del código fuente. El código fuente no es lo ejecutado por el procesador; existe uno o más intermediarios que transforman ese código fuente en código si se quiere ejecutable. Estamos haciendo referencia a los compiladores, intérpretes, vinculadores, etc. [13]. Los investigadores versados en el área de seguridad en sistemas rápidamente reconocen que es factible obtener un ejecutable adulterado a partir de un código fuente correcto, haciendo uso simplemente de un compilador o un intérprete alterado a tal efecto. La disertación de Ken Thompson en ocasión de recibir el Turing Award [16], máximo galardón en el mundo al que pueden aspirar un investigador en ciencias de la computación, gira casualmente en torno a lo difícil que resulta detectar este tipo de ataque.

Esto implica, en el contexto de los sistemas de voto electrónico directo, que no es suficiente con asegurar que el código fuente del programa sea correcto, es necesario a su vez auditar el proceso de construcción del ejecutable, lo cual implica a su vez que se debe tener acceso al código fuente del propio compilador que se utilice, a fin de garantizar que está libre del tipo de adulteraciones antes comentado. Una vez más, las técnicas de firma digital y de encriptado pueden ser utilizadas en este contexto para asegurar que la integridad del ejecutable no ha sido comprometida.

4. Conclusiones

Los sistemas de voto electrónico en general y los sistemas de voto electrónico directo en particular están en condiciones de proveer un conjunto provechoso de beneficios, simplificando tareas tediosas como el escrutinio primario o repetitivas como el registro de los votantes. No obstante, cambiar la forma en la que se conducen las elecciones incorporando este tipo de tecnología abre la puerta a nuevos riesgos no contemplados los cuales, en el peor de los casos, pueden ser explotados para llevar adelante un fraude.

En este sentido, el requerir que se haga uso de software libre dentro del sistema de voto electrónico directo, el cual por definición garantiza un conjunto de cuatro libertades esenciales, parece atender algunos de los principales cuestionamientos. El hecho de que el código fuente del software debe estar necesariamente a disposición de cualquier interesado en auditarlo parece una virtud esencial. Sin duda, a lo largo de este trabajo arribamos a la conclusión de que requerir se haga uso exclusivo de software libre es una condición absolutamente necesaria. Aceptar que se use software privativo es lisa y llanamente inconcebible.

Lamentablemente, el solo hecho de usar software libre no es suficiente para garantizar que el sistema resultante sea al menos tan seguro como sistema de voto convencional. Las mismas técnicas empleadas para atacar sistemas de software en general pueden ser usadas para vulnerar el sistema de voto electrónico directo. El requisitos de mantener la integridad y el anonimato de los sufragios resultan objetivos encontrados, cuyo cumplimiento requiere de hacer un uso correcto y preciso de las avanzadas técnicas de firma digital y encriptado asimétrico. En consecuencia, como línea de trabajo a futuro nos proponemos explorar el rol que estas técnicas han de desempeñar en este tipo de sistemas, analizando qué requerimientos adicionales a nivel de infraestructura hacen falta para alcanzar el objetivo antes comentado de preservar al mismo tiempo la integridad y el secreto de los votos.

Referencias

[1] Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Sys-*

tems, 2nd ed. Wiley, 2008.

[2] Busaniche, B., and Heiz, F. *Voto electrónico - Los Riesgos de una Ilusión*. Fundación Via Libre, 2008.

[3] Feldman, A. J., Halderman, J. A., and Felten, E. W. Security Analysis of the Diebold AccuVote-TS Voting Machine. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop* (2006).

[4] Harris, B. *Black Box Voting: Ballot Tampering in the 21st Century*. Talion Publishing, 2004.

[5] Kaufman, C., Perlman, R., and Speciner, M. *Network Security: Private Communications in a Public World*, 2nd ed. Prentice Hall, 2002.

[6] Kohno, T., Stubblefield, A., Rubin, A. D., and Wallach, D. S. Analysis of an Electronic Voting System. In *IEE Symposium on Security and Privacy* (May 2004).

[7] Kurose, J. F., and Ross, K. W. *Computer Networking - A Top-Down Approach Featuring the Internet*, 5th ed. Addison Wesley, 2009.

[8] Prince, A. *Consideraciones, aportes y experiencias para el voto electrónico en Argentina*. Editorial Dunken, 2006.

[9] Raymond, E. S. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O'Reilly, 2001.

[10] Rivest, R. L., Shamir, A., and Adleman, L. M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM 21*, 2 (1978), 120–126.

[11] Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. Wiley, 1996.

[12] Stallman, R. M. *Free Software, Free Society: Selected Essays of Richard M. Stallman.* GNU Press, 2002.

[13] Tanenbaum, A. S. *Structured Computer Organization*, 5th ed. Prentice Hall, 2005.

[14] Tanenbaum, A. S. *Modern Operating Systems*, 3rd ed. Prentice Hall, 2007.

[15] Tanenbaum, A. S., and Wetherall, D. J. *Computer Networks*, 5th ed. Prentice Hall, 2010.

[16] Thompson, K. Reflections on trusting trust. *Communication of the ACM 27*, 8 (Aug. 1984), 761–763.

[17] Tula, M. I., Ed. *Voto Electrónico: Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales.* Ariel, 2005.