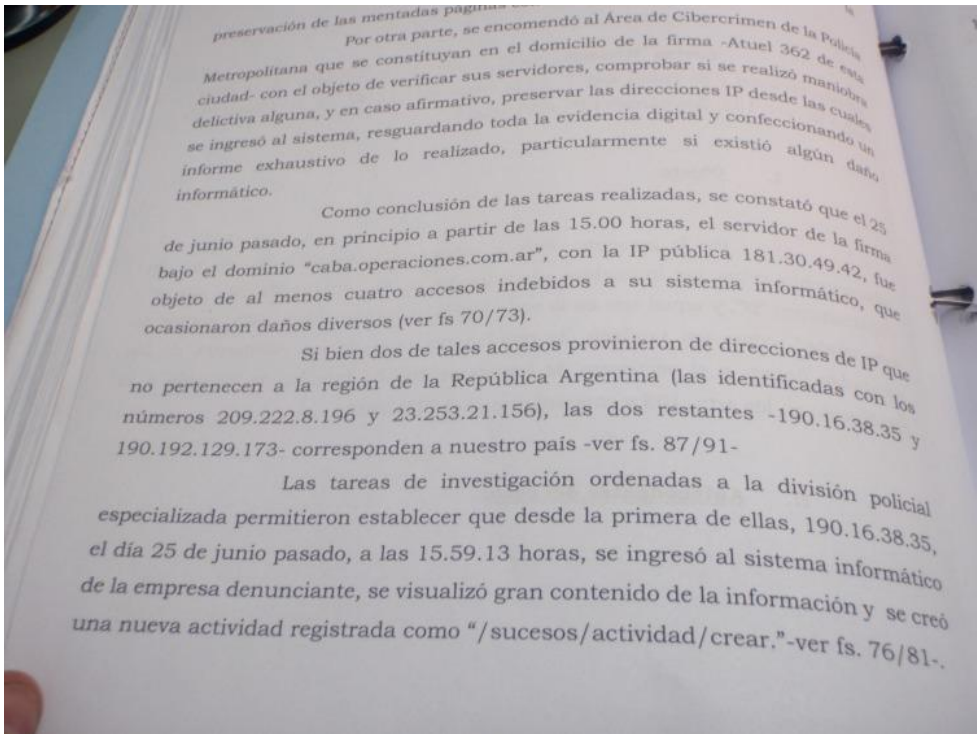
El voto hackeado: expediente muestra irregularidades en el voto electrónico en Capital Federal

Dos días antes de la elección de 2015 para Jefe de Gobierno porteño, un informe de la Policía Metropolitana confirmó un grave ataque informático a los servidores de la empresa Magic Software Argentina (MSA), que estaba a cargo de todo el proceso electoral. El dato es clave ya que revela que el sistema electoral basado en la Boleta Única Electrónica (BUE) fue infiltrado y que se hicieron modificaciones en el servidor que tenía que recibir los votos a pocas horas de la votación. Sin embargo, la jueza Maria Luisa Escrich priorizó la persecución de un supuesto delito informático frente a la protección de la voluntad popular que debía expresarse sin obstáculos en las elecciones.
Por esta investigación fue sobreseído hace pocos días el técnico informático Joaquín Sorianello, que simplemente advirtió las fallas en el sistema y avisó a la empresa MSA de las vulneraciones en su seguridad. Pero las pericias de la Policía Metropolitana que constan en el expediente revelan que el sistema que Mauricio Macri utilizó en la ciudad, a través del cual tuvo un triunfo político meses antes de las elecciones nacionales y que ahora quiere instrumentar a nivel nacional fue vulnerado por otras personas que llegaron a crear o eliminar “personas, delegados, técnicos, mesas y establecimientos” de votación y, por lo tanto, siembran dudas sobre el normal desarrollo de las elecciones porteñas.

Tomando en cuenta las pericias que constan en el expediente, las distintas auditorias sobre el sistema de BUE y la falta de control sobre MSA, es difícil garantizar la fidelidad absoluta sobre el resultado que finalmente otorgó la elección.

A confesión de parte

El 5 de julio de 2015 fue la primera vuelta en las elecciones para definir el Jefe de Gobierno porteño, con Horacio Rodríguez Larreta, Martin Lousteau y Mariano Recalde como principales candidatos. Dos días antes, la jueza Escrich ordenó allanar dos domicilios desde los cuales se había accedido en forma remota a los servidores que la empresa MSA utilizaría para la elección. Uno era el de Sorianello, el caso que tuvo repercusión mediática pero que fue finalmente sobreseído ya que quedó demostrado que en su acceso no generó ningún daño ni alteración al sistema de MSA. Sorianello simplemente hizo un PWONED, un concepto tomado del ajedrez que significa que un peón da jaque mate al rey, y que traducido al léxico informático da cuenta de que una persona encuentra una vulnerabilidad en una empresa y deja una marca. En este caso, Sorianello dejó una bandera en el sistema de MSA, que es inocua pero advertía de su fragilidad. Por las dudas, Sorianello incluso le advirtió a Felipe Llerena, empleado de MSA, de la falla de seguridad en su sistema, tal como consta en los registros de chat entre ellos anexados en el expediente.



preservación de las mentadas pági

Por otra parte, se encomendó al Área de Cibercrimen de la Policía Metropolitana que se constituyan en el domicilio de la firma -Atuel 362 de esta ciudad- con el objeto de verificar sus servidores, comprobar si se realizó maniobra delictiva alguna, y en caso afirmativo, preservar las direcciones IP desde las cuales se ingresó al sistema, resguardando toda la evidencia digital y confeccionando un informe exhaustivo de lo realizado, particularmente si existió algún daño informático.

Como conclusión de las tareas realizadas, se constató que el 25 de junio pasado, en principio a partir de las 15.00 horas, el servidor de la firma bajo el dominio "caba.operaciones.com.ar", con la IP pública 181.30.49.42, fue objeto de al menos cuatro accesos indebidos a su sistema informático, que ocasionaron daños diversos (ver fs 70/73).

Si bien dos de tales accesos provinieron de direcciones de IP que no pertenecen a la región de la República Argentina (las identificadas con los números 209.222.8.196 y 23.253.21.156), las dos restantes -190.16.38.35 y 190.192.129.173- corresponden a nuestro país -ver fs. 87/91-

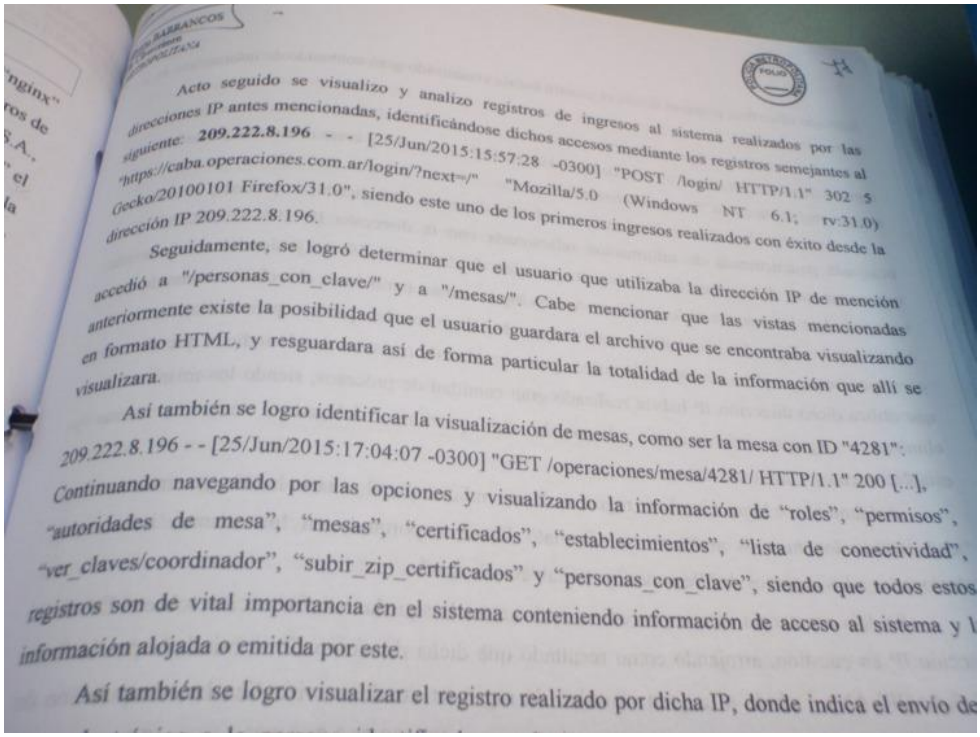
Las tareas de investigación ordenadas a la división policial especializada permitieron establecer que desde la primera de ellas, 190.16.38.35, el día 25 de junio pasado, a las 15.59.13 horas, se ingresó al sistema informático de la empresa denunciante, se visualizó gran contenido de la información y se creó una nueva actividad registrada como "/sucesos/actividad/crear."-ver fs. 76/81-.

Sin embargo, hubo otro caso que no trascendió. Se trata de Martin Leandro Manelli quien, según consta en el pedido de allanamiento de la fiscal Silvina Rivarola, “no solo visualizó numerosa información del sistema, sino que realizó procesos relacionados a la edición, creación y eliminación de información, tales como eliminar a la persona o establecimiento identificado con el ID 5210 y crear al Delegado con ID 3841”. Es decir, por un lado, Manelli hizo importantes modificaciones en el servidor donde se alojaba información electoral sensible. Por el otro, demostró la debilidad del sistema que, a fin de cuentas, debía garantizar la seguridad del voto de los porteños. De la lectura del expediente se desprende que Manelli no fue el único en vulnerar el sistema que Macri pretende implantar a nivel nacional.

La causa se inició el 1 de julio, es decir, cuatro días antes de la elección. Fue la propia empresa MSA, proveedora de las máquinas de votación y del servicio de conteo de votos, la que denunció accesos a su sistema informático. Fue una confesión de parte: la propia empresa evidenció la fragilidad de su sistema. Con un agravante: MSA aseguró que advirtió los ataques desde el 29 de junio, pero esperó dos días para denunciarlo. A su vez, en las pericias posteriores se demostró que los ataques informáticos ocurrieron varios días antes de la denuncia e incluso antes de la fecha que declaró MSA. Con las elecciones totalmente tercerizadas en manos de MSA, una falla en su sistema debía reportarse de inmediato ya que ponía en riesgo la votación.

Según consta en el expediente, en los accesos al sistema de MSA se obtuvo información que fue publicada en varios sitios de internet, incluyendo la nómina de los técnicos de la empresa que trabajarían el día de la elección. Los técnicos ni siquiera eran de MSA: fueron reclutados por Cider SA y RandStad, dos empresas dedicadas a la tercerización de recursos humanos. O sea: una elección tercerizada ejecutada por técnicos tercerizados. La publicación, por su parte, efectivamente existía, y se acusaba a los técnicos como posibles responsables de alterar los datos de la

votación. Para la empresa, la intrusión en su sistema encuadra como “daño informático”, según el artículo 183 del Código Penal. Al día siguiente, el 2 de julio, la fiscal Rivarola solicitó al Área de Cibercrimen de la Policía Metropolitana que comprobara lo denunciado por MSA y, en caso afirmativo, que elaborara un informe.



Acto seguido se visualizo y analizo registros de ingresos al sistema realizados por las direcciones IP antes mencionadas, identificándose dichos accesos mediante los registros semejantes al siguiente: **209.222.8.196** - - [25/Jun/2015:15:57:28 -0300] "POST /login/ HTTP/1.1" 302 5 "https://caba.operaciones.com.ar/login/?next=/" "Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0", siendo este uno de los primeros ingresos realizados con éxito desde la dirección IP 209.222.8.196.

Seguidamente, se logró determinar que el usuario que utilizaba la dirección IP de mención accedió a "/personas_con_clave/" y a "/mesas/". Cabe mencionar que las vistas mencionadas anteriormente existe la posibilidad que el usuario guardara el archivo que se encontraba visualizando en formato HTML, y resguardara así de forma particular la totalidad de la información que allí se visualizara.

Así también se logro identificar la visualización de mesas, como ser la mesa con ID "4281": 209.222.8.196 - - [25/Jun/2015:17:04:07 -0300] "GET /operaciones/mesa/4281/ HTTP/1.1" 200 [...],

Continuando navegando por las opciones y visualizando la información de “roles”, “permisos”, “autoridades de mesa”, “mesas”, “certificados”, “establecimientos”, “lista de conectividad”, “ver_claves/coordinador”, “subir_zip_certificados” y “personas_con_clave”, siendo que todos estos registros son de vital importancia en el sistema conteniendo información de acceso al sistema y la información alojada o emitida por este.

Así también se logro visualizar el registro realizado por dicha IP, donde indica el envío de

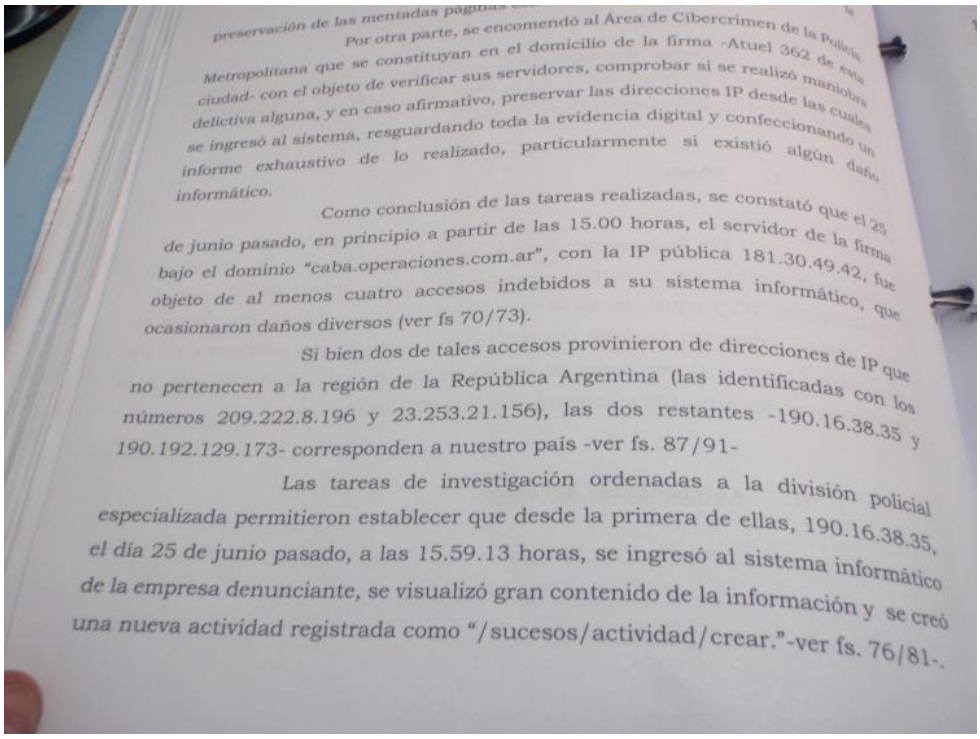
El mismo día el policía Javier Ezequiel Come fue a la sede de MSA en la calle Atuel 362 y presentó un informe que lleva la firma de su superior, el Comisionado Mayor Carlos Rojas, Jefe del Departamento Investigaciones Especiales y Complejas del Área de Cibercrimen. En ese primer informe se comprueba que el 25 de junio de 2015 los servidores de MSA, alojados en un datacenter ubicado en Florida 141, recibieron un ataque informático desde varios IP (los IP son el número de identificación de cada computadora) distintos entre las 18:57 y las 19:08hs. Es decir, el ataque no fue el 29 de junio como relató MSA en su presentación judicial, sino el 25. Eso abre dos opciones: o la empresa retaceó la denuncia al menos 6 días o su seguridad informática era tan frágil que tardó 4 días en advertir el ataque. En el informe consta que el propio dueño de MSA, Sergio Angelini, reconoce que ese servidor

“es el encargado de coordinar las tareas técnicas sobre los aspectos de las elecciones”.

Frente a este primer informe, la fiscal Rivarola solicitó más datos a Cibercrimen, que elaboró al día siguiente un segundo informe técnico más detallado que reveló graves vulneraciones al sistema de MSA. Este lo firman el Comisionado Mayor Rojas y el oficial Nazareno Monzón, y lo realizó el Oficial Mayo Alberto Horacio Barrancos. Algo destacable es que estos informes sólo los realizó la Policía Metropolitana ya que, aún a pocas horas de la elección, en el expediente consta que MSA le dijo a la policía que “ha adoptado las medidas técnicas necesarias para aislar el incidente y evitar que se repita, pero no tiene posibilidad de detener sus procesos internos ni asignar recursos específicos a la investigación”. Traducido, la empresa responsable de la votación no podía verificar cómo se violó su seguridad y que implicancias tenía.

Este segundo informe la Policía Metropolitana verifica “gran cantidad de registros donde indican la visualización de diferentes datos en el sistema, como así también su acceso, edición, eliminación y creación”. O sea, que quienes ingresaron al sistema de MSA pudieron modificarlo. Los ingresos se hicieron desde 5 direcciones de IP, 209.222.8.196, 23.253.21.156, 190.192.129.173, 190.210.205.193 y 190.16.38.35. Ésta última es el de Sorianello, ya sobreseído. Pero los demás, según el informe de Cibercrimen, no sólo visualizaron la información de los servidores de MSA sino que varios hicieron modificaciones o incluso generaron información. Todo esto, vale recordar, dentro del sistema que regía las elecciones porteñas. El IP 190.192.129.173, que corresponde a Manelli, además de visualizar numerosos datos del servidor logró editar la información de personas y permisos dentro del sistema, creó nuevas personas o establecimientos e incluso un nuevo Delegado. De las 5 IP, el informe policial destaca que hay 2 (las que empiezan con 209 y 23) que no pertenecen a la región de la Argentina. Ambas están localizadas en Estados Unidos, lo cual

abre dos hipótesis: o los accesos se hicieron desde allí, lo cuál implica un ataque externo al sistema de votación porteño, o podría tratarse de personas que utilizaron el programa Tor, un navegador de libre descarga que simplemente oculta la IP real. Como fuere, uno de estos ingresos desde un IP en Estados Unidos accedió zonas del sistema de MSA con el nombre de "personas_con_clave", "mesas", "autoridades de mesa", "establecimientos", "lista de conectividad", que, según el informe de la Metropolitana, "todos estos registros son de vital importancia en el sistema conteniendo información de acceso al sistema y la información alojada o emitida por este".



preservación de las mentadas páginas
Por otra parte, se encomendó al Área de Cibercrimen de la Policía Metropolitana que se constituyan en el domicilio de la firma -Atuel 362 de esta ciudad- con el objeto de verificar sus servidores, comprobar si se realizó maniobra delictiva alguna, y en caso afirmativo, preservar las direcciones IP desde las cuales se ingresó al sistema, resguardando toda la evidencia digital y confeccionando un informe exhaustivo de lo realizado, particularmente si existió algún daño informático.

Como conclusión de las tareas realizadas, se constató que el 25 de junio pasado, en principio a partir de las 15.00 horas, el servidor de la firma bajo el dominio "caba.operaciones.com.ar", con la IP pública 181.30.49.42, fue objeto de al menos cuatro accesos indebidos a su sistema informático, que ocasionaron daños diversos (ver fs 70/73).

Si bien dos de tales accesos provinieron de direcciones de IP que no pertenecen a la región de la República Argentina (las identificadas con los números 209.222.8.196 y 23.253.21.156), las dos restantes -190.16.38.35 y 190.192.129.173- corresponden a nuestro país -ver fs. 87/91-

Las tareas de investigación ordenadas a la división policial especializada permitieron establecer que desde la primera de ellas, 190.16.38.35, el día 25 de junio pasado, a las 15.59.13 horas, se ingresó al sistema informático de la empresa denunciante, se visualizó gran contenido de la información y se creó una nueva actividad registrada como "/sucesos/actividad/crear."-ver fs. 76/81-.

Con esta información, la jueza Escrich ordenó el allanamiento de los domicilios de Sorianello, que simplemente avisó a MSA de la vulneración, y de Manelli, que efectivamente hizo modificaciones en el sistema de las elecciones. Nada pudo hacer con los ataques desde el exterior, dato clave que revela la fragilidad del sistema. La jueza habilitó el allanamiento nocturno dada la cercanía de las elecciones, que se realizarían 2 días después, para impedir posibles ataques durante los comicios. En lo que no reparó la jueza fue en su propia contradicción: si tenía probada la vulnerabilidad

del sistema, más que allanamientos debía pensar en suspender las elecciones. Si hubo ataques durante las elecciones es un misterio: el sistema no fue auditado. Y es sabido que los ataques informáticos efectivos son, justamente, los que no se detectan. Mientas Macri insiste en llevar este sistema a las elecciones nacionales, la causa aún esta abierta.

Yo te avisé

El proyecto de Reforma Electoral que Macri envió al Congreso asegura: “las auditorias realizadas (…) permiten asumir que la boleta única con dispositivos electrónicos ha funcionado satisfactoriamente en los diferentes distritos en los que ha tenido lugar”. Esto es claramente falso.

Si el expediente judicial demuestra que la Policía Metropolitana reveló las vulneraciones de la seguridad del sistema que regía la votación, la revisión de las diversas auditorías previas a la elección confirman la fragilidad del sistema.

En las semanas previas a las elecciones porteñas hubo numerosas advertencias desoídas por el macrismo. El 5 de junio, justo un mes antes de la primera vuelta de la elecciones, el Tribunal Superior de Justicia (TSJ) porteño aprobó el sistema de voto electrónico. Los jueces Luis Lozano, José Osvaldo Casás, Ana María Conde, Alicia Ruiz e Ines Weinberg se ampararon en una auditoria realizada por el Departamento de Computación de la Facultad de Ciencias Exactas de la Universidad de Buenos Aires (UBA) que lleva la firma Claudio Enrique Righetti, docente universitario que es a su vez Jefe de Seguridad de Redes de Cablevisión, empresa del Grupo Clarín.

El encabezado de esta auditoría aclara que es un avance parcial de lo analizado hasta el 1 de junio, y esta plagada de contradicciones. Para justificar la aprobación del sistema de BUE, el TSJ cita fragmentos de esta auditoría parcial que están en su Resumen Ejecutivo: “De las tareas de auditoría llevadas a cabo

hasta la fecha no se han detectado problemas graves, ni indicios de que las observaciones que se describen a continuación puedan causar inconvenientes insalvables el día de la elección". Lo notable es que los jueces directamente descartaron los párrafos donde la auditoría, aún parcial, marca las falencias del sistema. La auditoría de la UBA reconoce que "no se audita el sistema de operaciones que la empresa utiliza para el seguimiento y control del operativo". Es decir, aún si el voto se emitía de forma correcta, el Tribunal autorizó el este sistema sin saber como se iban a trasmitir y contar esos votos.

Tampoco fueron relevados los lugares de votación "en cuanto a sus instalaciones eléctricas y la conectividad a internet", dato que salvaguardan con la existencia de baterías en las máquinas de votación. La misma auditoria parcial de la UBA afirma que la información con planes de contingencia ante problemas en la transmisión de los datos que presentó MSA "no cumple con las reglas del arte de una documentación de contingencia". A un mes de la votación, la auditoria parcial reveló que "el esquema de transmisión desde los centros de votación está aún en etapa de definición". O sea: se aprobó un sistema de votación sin definiciones centrales de su funcionamiento.

Esta auditoria también informó un dato inquietante: el Centro de Cómputos virtual que se utilizaría para la elección sería el gigante global Amazon a través de servidores en Brasil con un back up (resguardo) en Estados Unidos. En definitiva, la auditoria parcial sobre la que se basaron los jueces para autorizar la votación electrónica sólo evaluó aspectos superficiales del sistema, sin controlar parámetros de seguridad. Aún así, remarcó varias deficiencias del sistema que fueron desestimadas por el Tribunal a la hora de aprobar su uso.

El 14 de agosto de 2015, casi un mes después del ballotage que proclamó a Rodríguez Larreta como Jefe de Gobierno por apenas 54.855 votos de diferencia, el técnico de la UBA y Clarín Righetti

entregó la auditoría final del sistema de BUE. En esta auditoria final afirma que “el código fuente auditado tiene una gran cantidad de debilidades de distintos tipos”. El informe insiste: “lo que se ha observado es que el código fuente no sigue pautas de programación segura”. La auditoría también advierte que la configuración y generación del DVD que se introducía en la máquina para votar se hizo “utilizando un procedimiento que no estaba documentado ni fue auditado”. También muestra que hubo cambios entre la primera y la segunda vuelta que califica de innecesarios: “se observaron una cantidad de cambios en el código fuente entre la primera y la segunda vuelta mucho mayor a lo esperado, si se piensa que sólo estaba planificado cambiar las categorías a elegirse (…) y el diseño de pantalla”. Mas adelante, sostiene que “entre ambas elecciones (primera y segunda vuelta) se observaron cambios en la forma de encarar la seguridad y los procedimientos de trasmisión”. ¿Por que se modificó esta configuración para la elección entre Rodríguez Larreta y Lousteau, que terminó con un pequeño margen de diferencia? En la trasmisión de los datos de las escuelas al centro de cómputos estaba uno de los momentos más vulnerables de la elección. La auditoría revela que había problemas en los permisos para acceder a opciones de la máquina: “esto es riesgoso ya que ante una vulnerabilidad que afecte a cualquier parte del sistema, si se la logra explotar, es trivial que el atacante obtenga el control total del equipo”.

En las conclusiones de la auditoría final de la UBA afloran las contradicciones. A pesar de las advertencias a lo largo de los diversos informes, primero afirma que la utilización de BUE “fue exitoso y sin mayores sobresaltos”. Sin embargo, más adelante, confiesa que “todo el proceso de adopción, adquisición y auditoría fue hecho con demasiado apuro y con algún grado de improvisación, impidiendo que los procesos en general y la auditoría y la capacitación en particular, sean más efectivos”. O sea, si no se pudo auditar correctamente, ¿por que se aprobó el sistema?

La UBA no fue la única que advirtió sobre la BUE. El 10 de junio de 2015, luego de que el TSJ aprobara el sistema de votación, Ivan Barrera Oro y Lucas Lakausky participaron de una reunión en las oficinas de MSA para auditar el sistema. Luego presentaron un informe titulado “Vot.ar: una mala elcción” donde demostraron: que el chip RFID de la BUE puede ser leído por un tercero, que “la impresión térmica posee una vida media corta, anulando auditorías o revisiones futuras sobre un proceso electoral”, que se podía acceder a la máquina de votación y alterar su funcionamiento, todo lo cual mostraba que el voto no era ni secreto ni seguro y que el sistema no era trasparente. Concluyeron que “de no realizarse conteo/escrutinio/verificación manual, el resultado del sufragio queda vulnerable al fraude electoral” y por lo tanto “el sistema no cumple con los objetivos prometidos de brindar seguridad y transparencia y ocasiona un costo adicional al Estado, Ciudad o Municipio que lo emplea”.

Este informe llegó a manos de Julián Rousselot, hijo del ex intendente de Morón Juan Carlos Rousselot, aquel que en la década del 80 instrumentó un negociado alrededor de un plan de cloacas con el actual presidente. Al parecer Rousselot hijo, que afirma que lleva con orgullo su apellido, heredó el vínculo con Macri: desde el 10 de diciembre de 2015 es un asiduo visitante de la Casa Rosada. Rousselot hijo es Secretario General del Sindicato Único de Trabajadores Informáticos (SUTIRA), alineado con la CGT Azul y Blanca de Luis Barrionuevo. Tiene buena relación con el Secretario de Trabajo Ezequiel Sabor, dato no menor: el SUTIRA pugna con otros gremios por quedarse con la representación de los técnicos informáticos, cuestión que depende de la venia de Macri y Sabor. El 1 de julio de 2015, a cuatro días de la elección y el mismo día que MSA denunció la intrusión en su sistema, Rousselot participó como veedor informático de la audiencia de grabación de los DVD que se utilizarían en las máquinas de votación, en un depósito en la calle Bogotá 1650. En ese momento publicó: “hemos hecho un acto de fe del contenido, asumiendo que es correcto, hecho que en informática no es una práctica recomendada”. Por

entonces Rousselot tomó el informe de Barrera Oro y Lakousky como fuente principal para elaborar su propio informe junto a Solano Navarro, también dirigente del SUTIRA y precandidato a Diputado Nacional en Catamarca por el espacio de Barrionuevo. Este informe fue solicitado por Guillermo Laje, primo de Lousteau, que fungía como jefe de campaña y luego acompañó al novel embajador como Representante comercial. No fue el único informe crítico que recibió Lousteau sobre las irregularidades y falencias del sistema de BUE, pero finalmente aceptó el resultado electoral que lo dejó fuera de la jefatura de gobierno porteño pero lo catapultó a la embajada en Estados Unidos.

Este informe de Rousselot y Navarro señala, en principio, las mismas críticas: que el chip de las boletas se puede leer con un celular básico, que vulnera el secreto del voto y no debe utilizarse en elecciones; que la auditoría independiente se hizo sobre una versión de prueba del sistema de votación y, por lo tanto, no el que se utilizó el día de la elección; que las máquinas auditadas tenían puertos USB a la vista y, por lo tanto, con posibilidad de acceso a la computadora para hacer modificaciones; que incluso estaba mal configurado el día y hora. Rousselot y Navarro también reconocieron restricciones para realizar la auditoria y escribieron: “Vale aclarar que el análisis en el presente documento únicamente tiene validez en caso de que el sistema utilizado en las elecciones contenga el mismo código fuente que se auditó. No hay elementos que permitan evidenciar que el código que se utilizará en las elecciones corresponda con el código auditado; es decir, no se proporciona ninguna garantía sobre la ausencia de modificaciones en la versión final respecto a versión auditada”. Este informe remarca también los problemas posibles en la trasmisión de los datos de las escuelas al centro de cómputos, sobre el cuál no obtuvieron información.

Según Rousselot y Navarro, “la principal desventaja del sistema radica en el hecho de que el mismo es de código fuente cerrado, por lo cual no es posible para el público general validar la

autenticidad del código fuente del sistema ni de las librerías utilizadas. Adicionalmente, dado que el software no puede ser revisado por expertos independientes, la seguridad y autenticidad del sistema queda en manos de un número limitado de profesionales". A pesar de todos los problemas que enumeran, Rousselot y Navarro identifican ventajas en el sistema. Al afirmar que las máquinas de votación no guardan información, sostienen: "Por esta razón, gran parte del protocolo electoral se mantiene inalterado, y continúa siendo el principal elemento que garantiza la seguridad de los comicios. De esta manera, el sistema mejora parte del proceso sin perjudicar sustancialmente las medidas de seguridad existentes que caracterizan a los comicios". Más adelante, al referirse a la posibilidad de un fraude electoral, insisten: "Cabe aclarar que los riesgos de fraude se encuentran mitigados por el hecho de que el sistema no reemplaza los mecanismos tradicionales de seguridad en un comicio (por ejemplo la fiscalización del conteo de votos), al tratarse de un sistema de boleta electrónica y no un sistema completo de voto electrónico". Las contradicciones se hacen más evidentes cuando analizan el conteo de los votos: "el riesgo de un conteo incorrecto queda naturalmente mitigado por la posibilidad de fiscalización manual que permite el sistema, siempre y cuando el Presidente de mesa elija hacer un conteo manual, al contener las boletas información impresa que permite la fiscalización manual". O sea, si el presidente de mesa no hace el conteo manual, la elección depende de un sistema vulnerable. En el mismo informe, Rousselot y Navarro advierten que "la naturaleza misma del sistema genera un escenario en donde las posibilidades de fraude o manipulación son altamente probables debido a la naturaleza informática de la implementación". Pese a todo esto, en las conclusiones afirman que "los puntos de vulnerabilidad en lo que hace a la aplicación son limitados", para luego reconocer que "se concluye que en la versión que se presentó para el análisis no se ha encontrado código malicioso pero sí potencialmente vulnerable que pudiera alterar los resultados del proceso electoral".

Por último, revelan: “Cabe destacar la ausencia de mecanismos que garanticen que el código auditado sea el que se ejecute realmente en las elecciones. Al tratarse de una aplicación de código fuente cerrado, no existen mecanismos que permitan al público verificar la autenticidad del contenido de los DVDs, por lo que el funcionamiento final del sistema podría ser adulterado sin conocimiento de los auditores que han examinado el código fuente”.

Hay un tercer informe que no sólo refuerza las críticas de los anteriores sino que refuta las ventajas que plantean Rousselot y Navarro. Fechado en julio de 2015, fue realizado por un grupo interdisciplinario de especialistas integrado por Francisco Amato, Barrera Oro, Enrique Chaparro, Sergio Demian Lerner, Alfredo Ortega, Juliano Rizzo, Fernando Russ, Javier Smaldone y Nicolas Waisman. Desde el inicio, advierten: “los equipos utilizados en las elecciones no han sido certificados en ningún punto del proceso, situación que pone en jaque la seguridad del sistema. Consideramos que esta falla es del tipo crítica.” El informe es taxativo: “todos los elementos que hacen a las buenas prácticas del arte de la informática han sido omitidos”. Entre los puntos vulnerables insisten con el chip RFID donde se grabó el voto. Si bien MSA hizo correcciones para que el chip no pudiera ser modificado una vez grabado, no pudo evitar que cualquier personascon un celular pueda leer su contenido. Por lo tanto, viola el secreto del voto. MSA buscó salvar esta irregularidad con la colocación de una lámina metálica que evita la lectura al doblar la boleta para meterla en la urna. Pero este grupo de expertos demostró que si la lámina se separa del chip más de 8 milímetros ya habilita su lectura. El chip RFID fue descartado en Israel por sus problemas de seguridad. A pesar de que Macri y sus funcionarios aseguraron que las máquinas de votación eran simples impresoras, este grupo también descubrió que tenían una memoria “que le permite almacenar todo tipo de información, como ser p.e. el voto y una marca de tiempo”. Respecto a esta memoria, el informe destaca que “resulta imposible determinar qué acciones está

llevando a cabo durante el proceso electoral, situación que consideramos de gravedad crítica". Esta situación fue comprobada por varios fiscales durante las elecciones. Un ejemplo, durante el ballotage, fue la mesa 2188, en la Escuela N 19 Francisco Balcarce. Allí, Lousteau obtuvo 116 votos, Rodríguez Larreta 108 y hubo 12 en blanco.

El dato de la memoria es clave, ya que desmonta el argumento oficial de que se trata de simples impresoras. Estas máquinas, finalmente, quedaron en manos de MSA, y no se conoce ninguna auditoría que determine qué se hizo con esa información. Estos expertos demostraron a su vez la posibilidad de multivoto, "que consiste en alterar el contenido del chip RFID con el objeto de emitir más de un voto en una sola boleta. La simpleza de esta vulnerabilidad pone en evidencia la falta de profesionalidad respecto de las reglas del arte con que cuenta todo el sistema Vot.Ar". Esta es otra de las muestras de lo inseguro que fue el sistema por el cuál los porteños eligieron Jefe de Gobierno. Estos expertos aseguraron que "no es posible comprender la totalidad del funcionamiento del sistema sin poseer conocimientos técnicos avanzados, que muy difícil resulta afirmar que el mismo sea igualitario". Este fue el argumento de la declaración de inconstitucionalidad del voto electrónico en Alemania.

A todo esto se suma que MSA tuvo tercerizado todo el proceso de votación, desde las máquinas, la emisión del voto, el conteo, la trasmisión y la centralización en el centro de cómputos. Por lo tanto una falla de seguridad en el sistema no se puede detectar de un paso al otro. **Mal de nacimiento**

Muchas de las irregularidades en el sistema fueron expuestas ante los Diputados en las audiencias en las cuales se debate la aplicación de este sistema a nivel nacional, proyecto que Macri esta empeñado en llevar adelante. La experiencia en la ciudad de Buenos Aires indica que el sistema no sólo fue vulnerable sino que hubo irregularidades desde el inicio. El 13 de diciembre de 2013

Macri logró la sanción de la ley 4894 que estableció modificaciones en el régimen electoral. Tenía como antecedente la experiencia en Salta, cuyo gobiernador Juan Manuel Urtubey es uno de los principales impulsores de su aplicación a nivel nacional y en el ámbito informático lo sindican como lobbista de MSA. La idea de voto electrónico fue mutando.

El especialista Javier Smaldone traza la cronología de los cambios de nombre del sistema y afirma que “no parecen obedecer a una evolución tecnológica, sino más bien a las necesidades de comunicación (y de esquivar cuestiones legales) de sus impulsores”. Smaldone reconstruye que en 2008 la empresa MSA lo registró como “voto electrónico”, y en Salta la boleta estaba identificada de ese modo. La ley 4894 estableció la boleta única y dejó abierta la posibilidad de implementar el voto electrónico. Siguiendo a Smaldone, “la falta de definición precisa de ‘voto electrónico’ en el texto de la ley permitió que el Poder Ejecutivo, a través del decreto reglamentario 376/014, introdujera la utilización del sistema de la empresa MSA. Para ello, se inventó un nombre que a la fecha no existía (y no existe aún en el resto del mundo): boleta única electrónica, esquivando de esta forma el requisito legal”. La dinámica parece repetirse para su aplicación a nivel nacional. El nuevo ardid es hablar de “boleta electrónica”. Cambian los nombres, pero el sistema es el mismo, y los beneficiarios y as vulnerabilidades también.

Retomando las irregularidades en la ciudad, al mes de aprobada la ley 4894, el 13 de enero de 2014, se aprobaron los pliegos de la licitación, que se abrieron quince días más tarde. El costo de los pliegos fue de $150.000, lo cuál limitó el número de oferentes tanto por el precio como por la sospechas de preadjudicación a MSA. El servicio incluía 9500 máquinas (7500 mesas electorales, 1000 de reposición y 1000 para capacitación) con su instalación, capacitación a organismos públicos y soporte técnico en las distintas instancias electorales. A los siete días la licitación de preadjudicó a MSA, y finalmente el 20 de febrero se confirmó su

contratación por 216 millones de pesos, monto que incluía las PASO (finalmente realizadas con boleta tradicional) y la primera y segunda vuelta. La oposición denunció que la licitación estaba direccionada hacia MSA.

Mientras el Gobierno impulsa el tratamiento parlamentario, varias fuentes consultadas sostienen que el Ministro del Interior Rogelio Frigerio ya cuenta con un prototipo de máquina para la votación de Corea. De hecho, el ministro de Modernización Andrés Ibarra estuvo a principios de julio en el país asiático digitando los acuerdos. Según dejaron trascender desde el Ministerio de Modernización, para una elección a nivel nacional calculan comprar 120.000 máquinas con un costo de 48 millones de dólares. Al cambio a 15 pesos, esto da 720 millones de pesos.
