

“Si decís que tu sistema es invulnerable, sos un mentiroso”

Bibiana Ruiz y Juan Suárez



Joaquín Sorianello. Foto: Georgina García

“El sistema de seguridad era vago y podía ser vulnerado con facilidad” probablemente sea la afirmación más trascendente del dictamen de la Fiscalía en lo Penal, Contravencional y de Faltas N°7 que sobreseyó al informático Joaquín Sorianello (28). Tal como se lo comunicaron el lunes 1 de agosto, el informe se refiere a la seguridad del servidor, que sería el encargado de recibir los datos desde las mesas de votación de la elección a Jefe de Gobierno de la ciudad, con la cual Horacio Rodríguez Larreta obtuvo –nada más

y nada menos que— su primera victoria.

La causa tomó estado público el 3 de julio de 2015, cuando se llevaron a cabo dos allanamientos ordenados por la jueza María Luisa Escrich en respuesta a las denuncias realizadas por la empresa MSA –responsable de la implementación del sistema de voto electrónico en CABA– debido a los ataques recibidos en ese servidor los días previos a la elección. Uno de los que ingresó a dicho servidor fue Sorianello. Sin embargo, su acción –según consta en la documentación judicial (de estos días)– se limitó a comprobar la falta de seguridad del sistema y comunicárselo a la empresa.

El sobreseimiento no llega en un momento cualquiera: esta semana empieza en el Congreso el debate sobre el proyecto de reforma electoral impulsada por el macrismo, que entre varias cosas incluye la implementación a nivel nacional de un sistema de voto electrónico igual al utilizado anteriormente en CABA y en la provincia de Salta, conocido como “Boleta Única Electrónica”. También incorpora nuevos tipos penales al Código Electoral Nacional (delitos informáticos electorales), que amenazan con criminalizar miradas indiscretas sobre problemas de seguridad en el sistema. Nada más intimidatorio que una causa penal, como la que le iniciaron a Sorianello y cuyo proceso duró mas de un año. En el bar del Bauen, ZOOM entrevistó a Joaquín y a su abogado, Rodrigo Iglesias, por un lado contentos, por el otro, expectantes.

El proceso

¿Que perdiste a raíz de esta causa?

JS: Si perdí algo en estos trece meses es un poco la ingenuidad. Uno tiene su formación política, su entendimiento del mundo, y de golpe te topás con el poder real. De repente viene la policía a tu casa y puede tirarte la puerta abajo y llevarte tus cosas. Empezás a ver todo el trasfondo mafioso que hay -porque no fue muy limpio lo que me pasó- y te empezás a preocupar: ¿qué intereses toqué realmente? Después de reportar a la empresa hicimos una gacetilla de prensa con mi novia para comunicar lo que había pasado, porque para mí el tema era bastante crítico. Veníamos de un proceso muy largo en el que le estaban mintiendo a la población –diciendo que la máquina de votación era sólo una impresora, por ejemplo– y para vos que entendés un poco de esto, resulta muy burdo, realmente es una mentira. Entonces, ¿qué voy a hacer, reportar solamente a la empresa? No, hacemos una gacetilla de prensa, lo mandamos a un montón de periodistas. Al otro día escuché por radio la gacetilla y dije “uff, esto es serio”.

“Si perdí algo en estos trece meses es un poco la ingenuidad. Uno tiene su formación política, su entendimiento del mundo, y de golpe te topás con el poder real. De repente viene la policía a tu casa y puede tirarte la puerta abajo y llevarte tus cosas”

¿Tuviste miedo?

JS: Ya me había asustado muchísimo el día anterior, cuando confirmé que los certificados estaban ahí [Nota: por los certificados fácilmente accesibles en el servidor de MSA] y me dije ¿esto es un error o lo hicieron a propósito? Te empezás a hacer preguntas. Una elección mueve intereses, hay intereses enormes, creo que la reacción natural es el miedo, pero no digo el miedo paralizante, sino el miedo que te hace tomar conciencia de la gravedad del

problema.

¿Te sentiste vulnerable durante el proceso?

JS: Creo que cuando perdés tu derecho a la privacidad empezás a darte cuenta de lo importante que es. ¿Qué van a encontrar en mis computadoras? ¿Qué pueden poner? Encima, el día después del allanamiento a mi casa se publicó lo del escándalo enorme de Hacking Team (la empresa que vendía a los gobiernos un kit de herramientas informáticas para hacer espionaje), donde se filtraron muchos mails, y entre los lugares donde vinieron a ofrecer sus productos estaba Argentina. Para que te des una idea, con uno de los módulos que tenía ese kit, vos podés hacer esto: tenés a un militante social o político que no querés que ande libremente por ahí, bueno, esta herramienta permitía por ejemplo inyectarle archivos con pedofilia en su computadora. Después le hacés un allanamiento por pedofilia y la encontrás, y preparate porque esas causas son pesadas y si a eso lo levanta un medio, desde el punto de vista social, todo el mundo va a pensar “en algo raro andaba”. La informática se usa como una herramienta para la manipulación política, el estado de miedo generalizado es terrible, no sabés quién te puede estar espiando, hay que aprender a defenderse.

¿Cambió tu perspectiva sobre la tecnología?

JS: Yo era muy naïve como programador. Uno a veces, como un nerd, no sé da cuenta del impacto social que tiene lo que hace, pero cuando lo empezás a pensar... ¿Qué impacto social tiene una máquina de voto electrónico? ¿Qué impacto social tiene un programa para compartir archivos? Tiene un impacto enorme, no es solamente un juguete tecnológico que hacés, sino que moldea y

cambia la forma en que nuestra sociedad se mueve, entonces hay que hacerlo con responsabilidad, con una mínima conciencia de que no estás tirando tiros al aire que no le van a pegar a nadie.

“Una elección mueve intereses, hay intereses enormes, creo que la reacción natural es el miedo, pero no digo el miedo paralizante, sino el miedo que te hace tomar conciencia de la gravedad del problema”

¿Y no hay conciencia sobre esto?

JS: Muy poca, creo que una falencia enorme con los profesionales de la tecnología es que han sido educados para no cuestionar su trabajo desde la política. “Yo soy técnico y en política no me meto”. Y creés que no hacés política, pero todo lo que hacemos está atravesado por la política, hasta cuando eligís tu trabajo, también hacés política.

¿Cuál es la repercusión de todo esto?

RI: Principalmente vemos una falta de conocimiento técnico legal bastante grande, que asusta. Entre los políticos hay algunos que toman la posta, dicen vamos a juntarnos, pero a los más mayores les cuesta. Sus asesores se están capacitando de manera bastante rápida e investigan sobre esos puntos. Puntualmente vimos algunas cosas que a mí me gustaron, otras que lógicamente no. Entre las que sí me gustaron están: que puntualizaron estar en contra del voto electrónico, ver que el secreto del voto es vulnerado, ver que los sistemas de seguridad son vulnerados, también se habló de la causa de Joaquín y de que los niveles de seguridad son bajos y la seguridad, vaga. Quizás no le dieron tanta

bola a la parte ecológica del voto electrónico, que sinceramente es bastante importante.

¿Y cómo se cambia esa situación?

JS: Para mí es un laburo de difusión, de contar, de hablar sobre el impacto social de escribir software, de haber crecido atravesados por la tecnología, entender mejor nuestro tiempo y ser concientes de que las cosas tecnológicas pueden salir muy mal.



Joaquín Sorianello. Foto: Georgina García

Servidores inseguros

Volviendo a la causa, en la notificación del sobreseimiento se menciona la “vaga” seguridad del sistema de Boleta Única Electrónica. En relación a eso, ¿qué otros pronunciamientos hay sobre la seguridad del sistema dentro de la causa?

RI: Entre los puntos de pericia hay uno que es sobre los

certificados SSL, es decir, la seguridad que había en la transmisión de los datos entre las escuelas y el servidor que iba a contar los votos (que se hacía por internet). Básicamente, dicen que siendo tan importantes los datos que se estaban manejando -como los de un proceso electoral- utilizar certificados SSL gratuitos no es una práctica recomendada para este tipo de información sensible. También, con el evento [Nota: dejar escrito la palabra “PWONED” en un lugar vulnerable del servidor, como una bandera para dar aviso] que genera Joaquín, se demuestra su vulnerabilidad, que podías cambiar lo que quisieras.

¿O sea que el servidor tenía una seguridad que estaba por debajo de lo habitual?

RI: En realidad, no es lo habitual, es lo que las reglas del arte determinan para ciertos niveles de seguridad. Para un acto eleccionario tendrías que tener los sistemas de seguridad más altos que puedas tener al momento. Cuestión que no fue así. Quedó demostrado que no. Y sabemos que ese servidor estuvo operativo hasta el 20 de julio, por los registros de acceso que tenemos. No sabemos si ese servidor se utilizó en verdad el día 5 de julio o no [Nota: el día de la elección general a Jefe de Gobierno] y aún no sabemos dónde está físicamente ese servidor. Tenemos una copia espejo de un tiempo determinado de todo el servidor. Es lo único que aportó MSA a la causa.

“Para un acto eleccionario tendrías que tener los sistemas de seguridad más altos que puedas tener al momento. Cuestión que no fue así. Quedó demostrado que no”

¿Qué debería haber hecho la Justicia al tomar conocimiento de este

hecho?

RI: La Constitución garantiza derechos a cada individuo, entonces hay dos problemas. Les vulneré los derechos constitucionales que tienen los imputados, les saqué sus bienes, me los llevé para peritar. A uno no le encontré nada, lo tuve que sobreseer, pero también encontré que este servidor sí tuvo problemas y no paré la elección. Es decir, tuve la potestad de saber que había problemas. Yo creo que la fiscal debería haberse puesto a investigar. El juez no puede hacer nada que la fiscal no pida, salvo muchas excepciones, pero una de esas excepciones es el interés público general, y acá cuenta el interés público general.



Joaquín Sorianello y Rodrigo Iglesias. Foto: Georgina García

“Ethical hacking”

Antes de seguir con este tema, es necesaria una pequeña

digresión para evitar ofender a los hackers que lean esta nota. Para los hackers, decir “hacking ético” es tan absurdo como decir “cerrajería ética”: nadie presume que un cerrajero, por sus habilidades en la vulneración de cerraduras, deba necesariamente ser un delincuente. Existe cierta controversia sobre la definición de hacker, pero una gran mayoría entiende que es simplemente alguien que busca “la resolución de un problema de forma creativa, aprovechando las propiedades de las cosas de forma inesperada o sorprendente”. Se conoce como “Ethical hacking” al ataque a la seguridad de un sistema con el fin no de producir daños, sino avisar o reportar sobre sus vulnerabilidades. En relación a este tema, el sobreseimiento de Sorianello marca un hito importante.

Por eso Iglesias comenta:

“Vos tenés dos marcos: primero, el ethical hacking es legal siempre y cuando haya un contrato. Firmás un contrato, secreto de confidencialidad, te pago y te digo: ‘destrozá el sistema y mandame un reporte’. Y el lunes me decís: ‘tu sistema tiene este problema de seguridad, te lo arreglo por tanta plata’. Te doy la plata, cuando esté arreglado, demostrámelo y ya está. Eso siempre estuvo vigente. Ahora, otra situación que siempre estuvo vigente y nunca había pasado era que una persona ataque una empresa, encuentre una vulnerabilidad, deje una bandera, informe a la empresa y la empresa lo denuncie, porque lo que está haciendo es aumentarles sus parámetros de seguridad. Los delitos informáticos son todos dolosos, vos tenés que tener la intención y la voluntad de generar daño, y lo tenés que probar. Si hacés el ingreso, dejás el registro e informás a la empresa antes de que te denuncie, ya el hecho deja de ser doloso y pasa a ser culposo.

En ese sentido, ¿el fallo sirve o le da cierta garantía a quien realiza hacking

ético?

RI: Exactamente. Más allá del sobreseimiento de Joaquín, lo más importante es que el hacking ético sin contrato se puede realizar y no es punible.

¿Genera jurisprudencia?

RI: Sí, por supuesto.

¿Y qué pasa si se aprueba el proyecto de Reforma Electoral?

RI: Si la Reforma se aprueba hoy, así como está, Joaquín tiene una condena de dos a seis años con prisión efectiva. Y si yo me presento en una mesa de elecciones y digo: “soy técnico y sé un montón de informática”, me llevan preso por las dudas. Es una locura total.

Si la solución no es el voto electrónico, ¿cuál es?

JS: Yo creo que por un lado está la boleta única en papel, que es de lo mejor que hay por ahora, pero también creo que se puede aprovechar la tecnología para hacer crowdsourcing [Nota: colaboración abierta distribuida o externalización abierta de tareas], es decir, verificar colectivamente las planillas con los resultados, tener un sistema que entregue un streaming de datos para poder procesarlo y que cualquiera pueda hacer detección temprana de fraude en el escrutinio provisorio. Hay herramientas que pueden ayudar a que el proceso sea más transparente, pero se trata de que haya más actores, no menos; no sólo una empresa con su tecnología cerrada -una caja negra que nadie puede ver- metida

entre el votante y su voto, sino poner más gente alrededor para controlar. Las soluciones tecnológicas no tienen porqué ser complicadas y no hace falta que la tecnología sea necesariamente digital; es un concepto más amplio, básicamente encontrar una forma mejor de hacerlo. El tecno-optimismo de implementar el voto electrónico a mí y a mucha otra gente no le cierra para nada, porque los que vivimos desarrollando sistemas entendemos que son vulnerables. Yo no estoy exento de que alguien encuentre un error de seguridad gravísimo en lo que hago. Ojalá que si lo encuentra me avise a tiempo para que pueda arreglarlo. Pero si decís que tu sistema es invulnerable, básicamente sos un mentiroso.