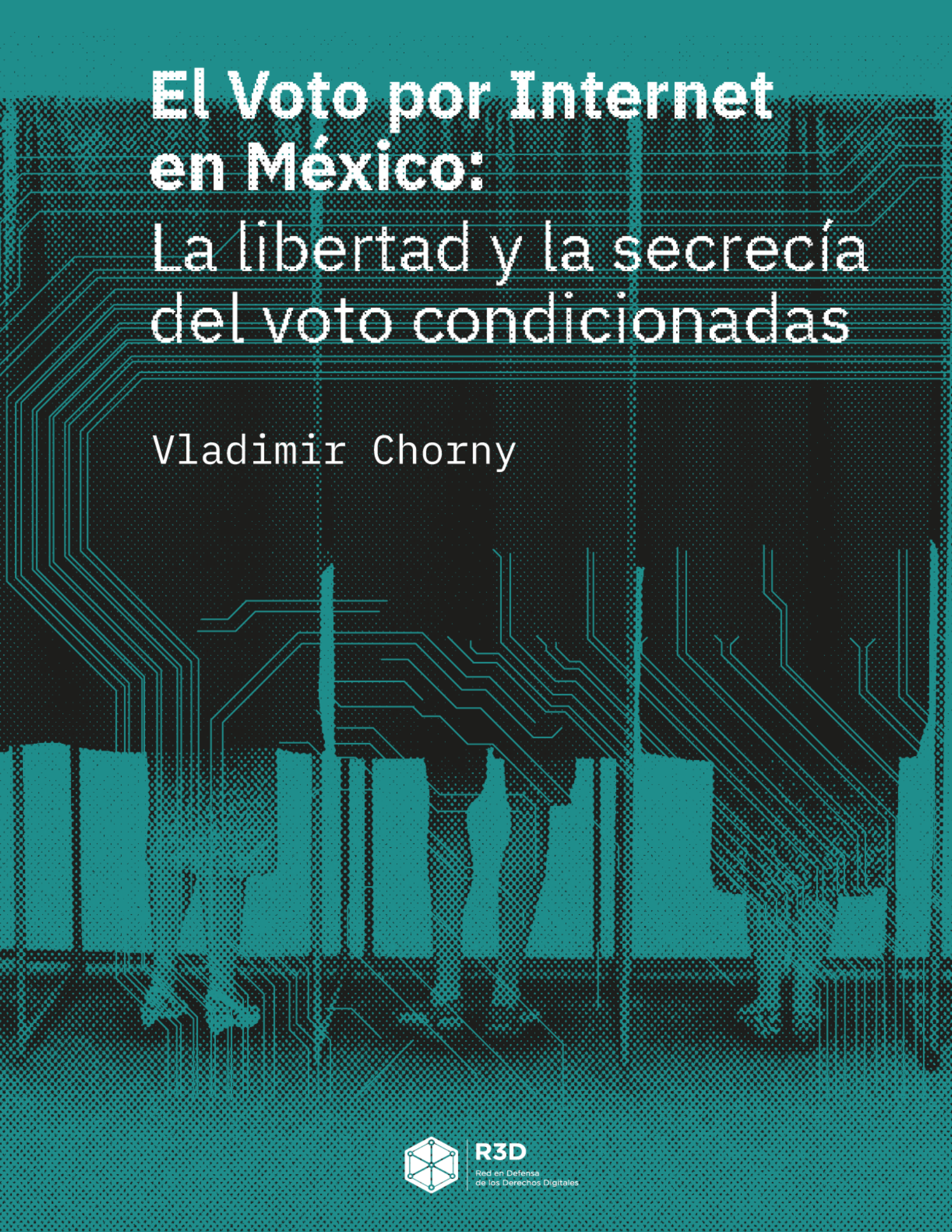
El Voto por Internet en México:
La libertad y la secrecía del voto condicionadas

Vladimir Chorny



R3D
Red en Defensa de los Derechos Digitales

EL VOTO POR INTERNET EN MÉXICO: LA LIBERTAD Y LA SECRECÍA DEL VOTO CONDICIONADAS

Por: **Vladimir Chorny**

Organización mexicana sin fines de lucro, dedicada a la defensa de los derechos humanos en el entorno digital. Utiliza diversas herramientas legales y de comunicación para hacer investigación de políticas, litigio estratégico, incidencia pública y campañas con el objetivo de promover los derechos digitales en México. En particular, la libertad de expresión, la privacidad, el acceso al conocimiento y la cultura libre.

Ciudad de México. México, octubre 2020

RESUMEN EJECUTIVO

Votar por Internet genera riesgos inevitables para las elecciones y para la democracia. Ninguna tecnología es infalible y, por el contrario, los sistemas de voto por Internet en todo el mundo son vulnerables a *hackeos* y, por ende, a fraudes electorales. Es importante ser muy claros en esto: no existe hoy y, probablemente no exista tampoco en el corto y mediano plazo, ninguna tecnología que pueda garantizar la certeza absoluta de un sistema de voto por Internet.

Desde el Pentágono hasta Google (pasando por la CIA y el Comité Nacional del Partido Demócrata) en los Estados Unidos de América (EUA), la historia de la seguridad informática revela una lucha constante en la mejora de mecanismos de seguridad y su permanente rompimiento o vulneración. Ni los organismos de seguridad más avanzados ni las empresas que más dinero invierten en tecnología de seguridad han logrado evitar ser *hackeados*, razón por la cual ninguno de ellos señala que su seguridad es infalible. Pero entonces, ¿por qué las autoridades en México aseguran que utilizar esta tecnología para votar es completamente seguro y garantiza la certeza, la integridad y la secrecía del voto (y de las elecciones)?

Los defensores del voto por Internet (en adelante VPI) ven estas tecnologías como el paso lógico a seguir en el camino de la modernización y el desarrollo de la democracia. Borrar las distancias materiales, quitar los cuerpos de en medio del ejercicio democrático y sustituirlos por computadoras y teléfonos inteligentes se plantea muchas veces como una panacea que agilizará la democracia y garantizará la legitimidad política de las elecciones. Ese último punto es sin duda correcto al menos en el siguiente sentido: en el voto por Internet lo que está en juego es tanto la seguridad de las elecciones como su legitimidad. Si los defensores del VPI se equivocan, la legitimidad de las elecciones y de los gobiernos electos en ellas y la credibilidad de las instituciones electorales están en un grave peligro.

Nuestra investigación analiza detalladamente los argumentos que suelen usarse a favor del VPI para evaluar su veracidad; explicamos los problemas principales del voto *online* y los riesgos que genera, a la luz de tres de las experiencias internacionales referentes en el tema (Alemania,

Estonia y los Estados Unidos de América); y, finalmente, revisamos críticamente el sistema de VPI de la Ciudad de México (CDMX) y del Instituto Electoral de la Ciudad de México (IECM), cuya última implementación (en marzo del 2020) fracasó y dejó a muchas personas sin la posibilidad de ejercer su derecho a votar.

1. Desmitificando al Voto por Internet

En las últimas dos décadas, algunos gobiernos y muchas empresas (interesadas por producir el *software* y el *hardware* que opera el sistema) han construido una serie de argumentos a favor del VPI. Curiosamente, cuando los analizamos de cerca nos damos cuenta de que o bien son empíricamente insostenibles o, en el mejor de los casos, cuentan a medias la verdad de lo que el voto por Internet significa para las elecciones.

A. No es cierto que el VPI aumente por sí mismo ni de manera necesaria la participación política

"Si la gente puede votar por Internet la participación política aumenta sin ninguna duda", es una frase común en las discusiones sobre las elecciones por Internet. El argumento asegura que al contar con una tecnología que remueve los obstáculos de acceso y tiempo (distancia, tiempo de espera, clima, etc.), un mayor número de personas va a votar porque el ejercicio democrático se vuelve menos exigente.

Más allá de si esto nos parece intuitivo o no, la afirmación es una cuestión de hecho, por lo que debe demostrarse empíricamente; el aumento en la participación no puede decretarse sólo porque la autoridad "cree" que ese va a ser el resultado. El problema es que de las experiencias internacionales y nacionales al respecto, no es posible desprender una conclusión como esta. Por el contrario, en muchos casos y por distintas razones (desconfianza en el sistema o en las autoridades, fallas técnicas o dificultades de uso), el resultado es el opuesto. La confianza, la usabilidad y otros factores (como la desigualdad estructural o la falta de educación

digital) hacen que, en el mejor de los casos, lo más que puede decirse de la participación es que la evidencia apunta en distintas direcciones.

En la investigación mostramos cómo en países como Suiza, Estonia y México (en el caso de la CDMX), no es posible sostener (sin mentir, al menos) que haya una relación causal entre la implementación del VPI y el aumento de la participación. El caso de la Ciudad de México es paradigmático porque no sólo hay evidencia que apunta en sentido contrario sino que, en las últimas elecciones realizadas con el sistema de VPI, el sistema falló dejando a muchas personas sin votar.[1]

B. El VPI no asegura la mayor practicabilidad y accesibilidad del voto

De manera similar, se dice que al votar desde la comodidad del hogar a través de teléfonos inteligentes o computadoras, el voto se vuelve más accesible y atractivo para las personas. Sin embargo, la realidad es que los sistemas de VPI varían mucho en su complejidad y que, de nuevo, el que sea más accesible y simple depende de factores externos que deben ser evaluados empíricamente. En el caso del sistema de la CDMX, el proceso de autenticación es complejo y requiere destrezas particulares; suele ser complicado de realizar para poder votar. El mejor ejemplo es que, el día que el sistema fue presentado a representantes de la sociedad civil en el IECM (enero 2020), el Consejero Electoral encargado de la prueba (familiarizado con él) tuvo que realizar el procedimiento varias veces, sin éxito, hasta que lo logró después de varios intentos y varios minutos invertidos en esa empresa.

Estas y otras dificultades (analfabetismo digital, desconfianza ante la dificultad del uso, etc.) cuestionan la afirmación a favor y muestran que depende de distintas variables. Otro problema concreto es que la mayoría de los países que usan el VPI no tienen estudios empíricos desagregados por sujetos y grupos que permitan medir de manera más confiable lo que

1. Al momento de cerrar la edición de la investigación, las elecciones en distintos distritos donde se utilizó el VPI habían sido impugnadas y estaban pendientes de resolución por el Tribunal Electoral de la Ciudad de México (TECDMX). Meses después, el TECDMX anuló varias de ellas precisamente porque el VPI falló y el derecho al voto de las y los ciudadanos de la CDMX fue violado.

las autoridades señalan. Ante la falta de información, no debemos olvidar que la carga de la prueba sobre los supuestos beneficios recae en las autoridades y que, en estos casos, no hay información suficiente que permita sostener lo que prometen.

C. No es seguro votar por Internet y ninguna tecnología hoy en día es suficiente para asegurar lo contrario

"Votar por Internet es completamente seguro y no implica ningún riesgo de seguridad". Los defensores del VPI aseguran que sus sistemas se apegan a los más altos estándares de seguridad informática y tecnológica y que las elecciones están fuera de peligro. Nos hablan de procesos de encriptación y protocolos criptográficos que garantizan la privacidad del voto al mismo tiempo que su seguridad y su integridad. Paradójicamente, tanto a nivel internacional como en México (en el caso del IECM), las autoridades suelen poner como ejemplo de la seguridad en Internet el hecho de que hoy en día realizamos operaciones bancarias por Internet o que pagamos productos y servicios en el entorno digital.

El ejemplo traslada de un plumazo el ámbito electoral al de los sistemas bancarios y comerciales, sin advertir las posibles incompatibilidades entre uno y otros. Los bancos no necesitan ser (y no lo son) democráticos, pero las elecciones sí. En el caso de la banca *online*, su funcionamiento tira en sentido contrario a la secrecía: todos los movimientos son registrados detalladamente y el monitoreo de los clientes es permanente para detectar posibles fraudes (y, con suerte, evitarlos). Aún así, los bancos pierden millones de dólares al año resultado de problemas de seguridad (fraudes, *hackeos*) que son imposibles de evitar sin importar la cantidad de dinero que destinen a ello (sus pérdidas son parte del modelo de negocios con el que funcionan). Tan sólo en el 2018, por ejemplo, las cifras oficiales muestran que en México hubo pérdidas de más de 13 mil 977 millones de pesos para ellos.

En el voto por Internet el problema es mucho mayor porque si una elección es manipulada (que haya un fraude) es muy difícil o incluso imposible saberlo. Cuando somos víctimas de un fraude en el banco, nos

damos cuenta porque podemos detectar movimientos que no realizamos o porque, sencillamente, el dinero desaparece. Pero con el voto por Internet no es posible darnos cuenta porque la tecnología y la naturaleza de los *software* que se usan para votar permiten manipular una elección (en caso de ser *hackeada*) sin dejar rastros; los fraudes electorales en Internet pueden ser invisibles.

Por ello, es importante entender que el VPI tiene todos los riesgos de las elecciones tradicionales como los conocemos (fraude interno, compraventa de votos, etc.) más los riesgos específicos que corresponden a la tecnología. Para comprender mejor lo que esto implica podemos pensar el universo de riesgos en dos grupos: *los relacionados con los votantes (o usuarios), y los relacionados con el sistema de VPI o sus servidores.*

Los riesgos de los usuarios son todas las formas en las que el voto o la información de las votantes pueden ser robados o manipulados, así como las maneras en que se puede ganar control del sistema de votación a través de los dispositivos de las personas. Primero, tenemos **la coerción.** El voto por Internet implica que las personas dejen de votar en el espacio creado para dar seguridad y privacidad para votar libremente, para que puedan votar "desde la comodidad de su hogar". Sin ese espacio seguro, las personas quedan a merced tanto del espacio privado (donde el Estado no está presente) en que habitan como de las distintas formas en que pueden ser coaccionadas (un esposo o padre que presiona a votar de alguna forma, un empleador, etc.).

En segundo lugar está el ***hackeo* de dispositivos a través de *malware*** o *software* malicioso con el que un atacante puede tomar control del teléfono inteligente o la computadora y cambiar el voto sin que el usuario se dé cuenta. Todo esto sin importar que el sistema esté encriptado, ya que el cambio del voto se hace antes de que la persona emita el voto, volviendo la encriptación "irrelevante" en este sentido. Hoy en día es relativamente simple infectar un dispositivo y es casi imposible darse cuenta de que el voto fue cambiado.

Por otro lado, el grupo de riesgos relacionados con el sistema pueden ser tanto **internos como externos.** Los internos son aquellos en los que una

autoridad electoral u otro sujeto relacionado con el armado del *software* o *hardware* pueden infectar el sistema para realizar un fraude. La diferencia con los fraudes tradicionales es importante: con el VPI, una sola persona dentro del sistema es suficiente para manipular la elección y realizar un fraude. Si, por ejemplo, alguien que opera el sistema o tiene acceso a las memorias USB o las computadoras o a algún componente utilizado en la elección, utiliza un virus e infecta el sistema, eso es suficiente para realizar el fraude y comprometer la elección.

Los riesgos externos son las formas de romper la seguridad de un sistema por atacantes externos a las autoridades que realizan la elección, particularmente sobre los servidores del sistema. Los servidores funcionan en distintos momentos de la elección para distintos propósitos (almacenar los votos encriptados, trasladarlos, descifrarlos, contarlos, etc.) y pueden ser atacados en distintos momentos y formas. Pueden realizarse, por ejemplo, **ataques de denegación de servicio (DDoS)**, para impedir que el sistema funcione y las personas puedan votar; ataques para robar información (tales como los de Amenaza Persistente Avanzada o Advanced Persistent Threat o APT), para robar información delicada o tomar el control del sistema; ataques de intermediario (conocidos como "man-in-the-middle attack") para robar las credenciales y cambiar el voto, entre otros.

Nada de esto es teórico o hipotético. Está demostrado y ampliamente estudiado que estos riesgos existen y que tienen costos reales. Sólo por señalar algunos ejemplos, el Pentágono y la CIA, al igual que Google, han sido víctimas de varios de estos ataques y han perdido información valiosa o visto sus sistemas comprometidos de distintas formas. Esto explica por qué este mismo año las principales agencias de seguridad de este país, tales como el FBI y el Departamento de Seguridad Nacional, **advirtieron a los Estados que votar por Internet era altamente peligroso y que debían abstenerse de hacerlo,** luego de que instituciones del más alto nivel especializadas en seguridad informática y en ciencias de la computación y tecnologías, tal como el MIT (*Massachusetts Institute of Technology*), advirtieron los riesgos y rechazaron la idea de implementar el voto *online*.

El problema es peor mientras más poder y dinero están en juego: mientras más poder económico y/o computacional tiene el atacante, es

más probable que pueda romper la seguridad y manipular una elección (sin que sea posible saberlo).

D. La naturaleza del voto por Internet impide garantizar la secrecía del voto y su integridad al mismo tiempo

Anteriormente mencionamos que si una elección es manipulada es casi imposible (o imposible) darnos cuenta de ello. Esto es así porque el voto por Internet lleva a un callejón sin salida que en la doctrina se conoce como "el dilema secrecía-integridad", que significa que las medidas que sirven para proteger la secrecía del voto atentan directamente contra las medidas necesarias para verificar su integridad.

Para proteger el secreto del voto, los sistemas separan la identidad del votante del sentido en que vota (la candidata que eligió, por ejemplo); es decir, que una vez que la persona vota en Internet, el programa de votación desvincula su nombre de su voto y luego envía el voto encriptado a una urna electrónica. En Internet, la materialidad del voto no existe; cada voto es meramente información procesada por el programa, y la persona debe confiar en que su voto se registró como ella indicó en la app para votar (counted as cast). Se trata de un acto de fe porque, a diferencia de las votaciones en papel donde las personas saben que el sentido de su voto se mantiene porque lo depositan personalmente en una urna que está protegida y vigilada durante todo el proceso hasta su conteo (y que ese voto será contado si hay necesidad de recuento), en el VPI todo sucede dentro de un programa que no vemos funcionar y que actúa de acuerdo a como es programado (y puede actuar diferente si se programa para ello).

Las medidas que protegen la integridad del voto, por otro lado, tiran en dirección contraria a las de la secrecía. Acciones tales como dar un recibo con el sentido del voto una vez que la persona votó, ponen en riesgo la secrecía porque cualquier persona que vea u obtenga ese papel puede ver cómo voté. Por eso normalmente los sistemas de VPI sólo dan un recibo que indica que el voto "fue registrado" por el sistema. Una vez más, la única opción que le queda al votante es confiar en que el sistema hace lo que las autoridades dicen que hace y, además, en que éste no será *hackeado* (desde fuera o desde dentro).

Por esta razón, si alguien cambia los votos de una elección al realizar un fraude (infectando con un *software* que cambia los resultados), nunca veríamos que los votos cambiaron porque el sistema funciona como una caja negra en la que sólo vemos los resultados. Si alguien exige un recuento, por ejemplo, el sistema de recuento es parte del mismo sistema que es vulnerable al riesgo de *hackeo*, por lo que es inútil usarlo si el sistema fue comprometido (las elecciones sin respaldo en papel no pueden auditarse manualmente). Por ello los fraudes en el VPI son, en este sentido, invisibles.

Comprender que la naturaleza de los sistemas de Internet significa que estos son programados para hacer lo que les dicen y que, por ende, pueden programarse para hacer otra cosa, nos sirve para entender no sólo por qué un fraude puede ser indetectable (una vez que el atacante se apodera del sistema puede manipularlo y después borrar sus huellas para mostrarlo como si estuviera íntegro) sino también por qué varias de las medidas que se toman para verificar que el sistema funciona bien son de carácter estético. Por ejemplo, cuando se abre una votación por Internet y se ve que no haya ningún voto emitido (que el conteo esté en cero) para "verificar que el sistema está íntegro" o "no ha sido manipulado", bien puede suceder que el sistema esté bajo control de un atacante y se le haya programado para mostrar un conteo en cero o para mostrarse íntegro aunque esté en el poder de quien va a realizar el fraude de la elección.

Nada de esto, tampoco, es hipotético. En varios de los principales países donde votan por Internet, todas las veces que expertas y expertos independientes revisaron íntegramente los sistemas de VPI pudieron romper la seguridad y exponer las vulnerabilidades (Estonia 2011 y 2015; EUA 2020 y en otras ocasiones como en Washington D.C. en el 2012; Australia 2017, tan solo por señalar algunos casos).

E. Hay serios problemas de transparencia y publicidad en el VPI

Otra promesa de las elecciones por Internet es que son auditables en su totalidad y que sus procedimientos pueden ser visibles y evaluados por completo. Sin embargo, esto pocas veces es verdad por tres razones.

Primero, porque normalmente (y así sucede en el caso mexicano), las auditorías están centralizadas y sectorizadas por las autoridades electorales, lo que hace que el sistema no pueda ser revisado de forma independiente por expertas y expertos externos al proceso. Así, el código del sistema usualmente no es abierto (*open source*), lo que impide la investigación completa del código fuente del *software* y sus componentes. ¿Cómo debería ser la auditoría? A nivel internacional, se realizan dos procesos conocidos como "pruebas de penetración y recompensa" e "ingeniería inversa", que permiten verificar la seguridad del sistema y ver qué tan fuerte es. En México debemos resignarnos a confiar en auditorías que muchas veces no revisan la totalidad del sistema o lo hacen desde un enfoque incorrecto.

Segundo, porque las auditorías que tenemos no son totalmente transparentes. Históricamente, los hallazgos de la auditoría en cuestiones de seguridad y de funcionamiento son comunicados de manera separada a la unidad técnica del Instituto y no son públicos (esto se demuestra en las auditorías del IECM). Todas las auditorías, siempre, han registrado errores o fallas en los niveles de seguridad o de funcionamiento, pero la información al respecto no está a disposición del público en general para su conocimiento. Además, existen acuerdos de confidencialidad que llevan a que esta información se comunique de manera privada. Esto es particularmente relevante para el caso del sistema del IECM: en la última elección el sistema falló (y las auditorías también), pero por la falta de transparencia no podemos saber qué información existía al respecto.

Tercero, porque las auditorías tienen un enfoque sobre la funcionalidad del sistema más que sobre los escenarios de riesgo y los tipos de atacantes que pueden manipular el sistema. No realizan, por ejemplo, análisis completos donde evalúen escenarios en los que existe un atacante con un alto poder computacional y económico que pueda burlar la seguridad del sistema. La ausencia de un enfoque de seguridad, sumada a la imposibilidad del análisis independiente hacen que el VPI quede exento del escrutinio público; que se vuelva una caja negra sobre la que sólo conocemos algunas cosas de manera muy general A diferencia de las elecciones tradicionales (donde quien quiera puede observar y verificar), sólo algunas personas saben a ciencia cierta cómo funciona y qué tan peligroso es.

El voto por Internet tiene otro problema inherente a su tecnología: comprenderlo a detalle requiere de conocimientos técnicos que son altamente especializados, relacionados con las ciencias de la computación, la tecnología y los procesos de encriptación. La complejidad de entender la programación para después poder confiar en que el sistema hace lo que hace, es un obstáculo para que las personas entiendan el sistema electoral. Cuando el obstáculo se suma a los demás problemas de transparencia, lo único que queda, nuevamente, es confiar en que el sistema hace lo que las autoridades dicen que hace. Pero esto no es suficiente para cumplir con los principios de publicidad, transparencia y certeza.

F. La economía del VPI depende de factores que no son evaluados

El optimismo tecnológico del voto por Internet suele sustentarse en el discurso de la reducción de costos (ahorrar en recursos humanos, producción de boletas, etc.). No obstante, los costos de establecerlo no deben evaluarse sólo por el valor del *hardware* y el *software* que se utiliza en el sistema, sino también por su reemplazo, modificación y revisión permanentes, así como por su actualización, capacitación de funcionarios y los gastos de auditorías, educación digital y comunicación ciudadana sobre su uso.

Como no hay una metodología estandarizada a nivel internacional sobre la que exista consenso sobre cómo medir estos costos, la conclusión de si es o no más económico depende de lo que se tome o no en cuenta. Un ejemplo es el de los “costos escondidos” del sistema, que son difíciles de evaluar e incorporar a la medición o que no contabilizan elementos preexistentes en los que el sistema se apoya (como la infraestructura) pero que deben ser revisados, adecuados y actualizados para mantener la seguridad del mismo.

Finalmente, el costo de un sistema debe evaluarse en proporción al número de votantes que lo utilizan, lo que significa que si un sistema es utilizado por muy pocas personas, su rentabilidad disminuye, por lo que la variable de la participación se vuelve relevante para evaluar la del costo. En el caso de la CDMX, la investigación muestra la poca participación y una

relación de votantes con el costo del sistema que no deja para nada claro que este argumento cumpla lo que promete. Además, cuando el sistema falla, el gasto del sistema es un extra porque normalmente debe sustituirse por boletas de papel como repuesto (a riesgo de que las personas pierdan la posibilidad de ejercer su derecho a votar). Esto fue justo lo que pasó en las últimas elecciones en las que se utilizó el VPI en la CDMX.

G. La eficiencia del VPI no es lineal; el error humano no es inaceptable

El argumento de que el voto por Internet permite realizar elecciones de manera más eficiente tampoco debe evaluarse de manera unidimensional, particularmente en el caso de tecnologías que son complejas. Si bien es cierto que las tecnologías implican un avance para realizar procesos y corregir errores humanos, de esto no se sigue necesariamente que toda una elección deba pasar a la modalidad *online*. Los sistemas de VPI pueden fallar y fallan (nuestro caso de estudio es prueba de ello), pero además, es frecuente que las y los funcionarios públicos que deben utilizarlos y participar en las jornadas no estén suficientemente capacitados para que la elección se lleve a cabo de manera eficiente.

A diferencia de los procesos que se siguen en las elecciones presenciales basadas en papel (donde existe una larga historia de capacitación y aprendizaje ciudadano), cuando un servidor falla, o cuando el *software* no funciona (tal como pasó en la elección de la CDMX), el sistema en su totalidad se paraliza. La eficiencia, por así decirlo, se pierde. El gran problema aquí es que corregir las fallas normalmente conlleva modificar partes del sistema que fueron previamente auditadas y que no son auditadas en ese momento, abriendo ventanas de riesgo de manipulación y fraude del sistema.

La indiscutible relevancia de la tecnología para complementar la acción humana no obliga a sustituir del todo los procesos analógicos sólo porque existen los errores humanos. Hoy en día, sin la necesidad del voto por Internet, muchos procesos y pasos de las elecciones basadas en papel ya incorporan el uso de la tecnología sin el costo de tomar todos los riesgos que implica el VPI.

Los errores humanos no tienen la gravedad que se les asigna; durante décadas, las autoridades electorales y las sociedades democráticas han mejorado sus sistemas y han creado procedimientos de revisión, observación y recuento que garantizan que el error humano no sea un problema serio para cuestionar la legitimidad de las elecciones ni los resultados electorales. Esto es así en gran parte porque cuando los humanos fallan, el error es visible y puede ser evaluado imparcialmente e, incluso, corregido por un Tribunal Electoral que revisa si esos errores son suficientes para poner en riesgo un resultado. El VPI es radicalmente distinto, primero porque no podemos ver los errores (o manipulaciones) en caso de que los haya y, segundo, porque si llega a haberlos, un solo error es suficiente en algunos casos para tomar control del sistema y manipular por completo una elección.

2. La experiencia comparada: la evidencia sobre los riesgos del voto por Internet

Las experiencias de Alemania, Estonia y EUA sirven de base para contextualizar los principios normativos más importantes sobre las elecciones y el voto en el entorno de Internet. El voto electrónico en general y el voto por Internet en particular no son nuevos, y el recorrido que tuvo en varios de los países referentes para la materia es útil para dar contenido concreto a los principios de publicidad, transparencia, certeza, seguridad e integridad del ejercicio democrático.

→ Alemania es uno de los países que abandonó la implementación de las modalidades electrónicas de votación. En el año 2009, el Tribunal Constitucional Alemán consideró que el sistema propuesto violaba distintos principios constitucionales porque no podía ser **controlado por el público, no había sido revisado de forma independiente y porque su código fuente era cerrado.** El Tribunal estableció dos principios que debían cumplirse siempre para asegurar que la modalidad de votación era compatible con los principios democráticos: 1) *El principio de publicidad,* que exige que todos los pasos esenciales de la elección estén sujetos al escrutinio público; y 2) *el principio de control ciudadano,* que implica que las personas

entienden los pasos del acto electoral en relación tanto al *software* como al hardware; es decir, que comprenden, **sin necesidad de conocimientos técnicos especiales**, cómo funciona el sistema de y la manera en que se obtienen los resultados.

En este caso existieron auditorías centralizadas por la autoridad electoral (tal como sucede en México), a partir de las que las autoridades señalaban que para garantizar la certeza y seguridad del sistema, era suficiente con que las personas tuvieran un recibo de que su voto se había recibido, que la junta electoral observara el proceso y que la unidad técnica hubiera analizado el *hardware* y el *software.* El Tribunal rechazó ambos argumentos a la luz de las obligaciones de publicidad y transparencia: los principios obligaban a que el sistema estuviera abierto a pruebas de penetración y recompensa de carácter independiente, ingeniería inversa y la publicación de toda la información relacionada.

La figura de la auditoría debía ser entendida de **manera amplia,** sin limitarse al control de instituciones públicas ni de entes designados por las autoridades. Además, el control ciudadano conllevaba la participación del público en la supervisión de los aparatos electorales en las distintas etapas de la elección, y no sólo cuando se emitía el voto. La ciudadanía debía tener todos los elementos necesarios y suficientes para "examinar por sí misma el funcionamiento correcto del sistema". En este sentido, **ni la palabra de las autoridades ni de los entes públicos pagados para hacer las auditorías era suficiente** para garantizar los principios electorales en juego.

El Tribunal señaló, finalmente, que el voto electrónico tiene el riesgo de la invisibilidad de sus errores y de las manipulaciones del sistema en caso de ser comprometido, por lo que hacía más fácil afectar toda una elección y más difícil darse cuenta de ello. Por ello también la auditabilidad del sistema debía ser total e independiente, sin restricciones en cuanto al código ni al sistema en general.

→ Estonia es el país referente del voto por Internet a nivel mundial. Lo ha usado por casi dos décadas y está implementado en sus elecciones nacionales de manera regular (es decir que no sólo lo usan para el voto en el extranjero), por lo que sin duda es el caso paradigmático del VPI en la actualidad.

El sistema de Estonia estuvo cerrado a la evaluación independiente (las pruebas de penetración y recompensa, la ingeniería inversa y el estudio completo del código y de los demás elementos del sistema) durante casi 10 años (en los que sí hubo auditorías controladas y centralizadas por el gobierno). Fue recién en el año 2011 cuando el gobierno permitió una investigación independiente de manera parcial, con resultados desalentadores que fueron ignorados por las autoridades. Posteriormente en el año 2014, el gobierno intentó reivindicarse e invitó a expertas y expertos independientes de distintos países para que estudiaran casi por completo el sistema, con la posibilidad de realizar ingeniería inversa. ¿Cuáles fueron los resultados?

El informe independiente coincidió y reforzó los hallazgos encontrados en el informe del 2011, señalando tres puntos alarmantes: 1) el proceso de anonimización del voto dejaba la posibilidad de romper la **secrecía** del voto porque no había forma de probar que las copias de la identidad fueran borradas; 2) el sistema de **seguridad** estaba lleno de riesgos: el informe señaló la facilidad de infectar los dispositivos con *malware* específicos, que permitían después hacer ingeniería inversa al tomar el control del cliente para después ganar el control de la elección. Además, los servidores tenían vulnerabilidades graves que permitían ganar fácilmente el control de la elección; 3) el sistema no era **transparente** como para poder evaluar por completo el código, ya que existían limitaciones sobre qué evaluar, y porque se establecían obligaciones de confidencialidad que evitaban poner los hallazgos en conocimiento del público.

La respuesta de las autoridades fue la misma que en el año 2011: decir que el sistema era seguro y confiable, que cumplía con los principios electorales y que garantizaba la certeza del resultado electoral (sin refutar ninguno de los señalamientos empíricos). Al hacerlo, replicó una práctica común de las autoridades electorales (probablemente más por desconocimiento de las tecnologías que por mala voluntad o intereses políticos): la de determinar la seguridad y la integridad del sistema de VPI por vía declarativa; es decir, señalar que el sistema es seguro y hace lo que hace sin importar los señalamientos en contrario ni la falta de investigación al respecto.

→ Estados Unidos de América es otro caso fundamental para entender al voto por Internet porque cuenta con experiencias locales en las que se probó (para luego desistir) y porque en el contexto de la pandemia causada por el COVID-19 existió un nuevo intento por establecerlo, para que las personas pudieran votar sin exponerse a los contagios. Esto llevó a que las principales agencias de seguridad del gobierno emitieran un comunicado a los Estados advirtiendo que se abstuvieran de votar por Internet debido a los altos riesgos que implicaba (con el resultado de que al menos uno de ellos frenó su implementación).

En el año 2010, el gobierno de Washington, D.C., abrió por primera vez su sistema de VPI, asegurando que era totalmente seguro e invitando a especialistas y expertas a que lo probaran e intentaran vulnerarlo (avalaron realizar pruebas de penetración y recompensa y hacer uso de ingeniería inversa con el código abierto). El resultado fue que un grupo de expertos no sólo *hackeó* el sistema para cambiar los votos y tomar control total del sistema sin que las autoridades se dieran cuenta, sino que lograron que las autoridades desistieran de usar el sistema en esas elecciones (a menos de una semana de celebrarse).

El voto electrónico en general y el voto por Internet en particular han sido fuertemente criticados en EUA desde hace años y existe mucha información disponible sobre los problemas tecnológicos relacionados con las ciencias de la computación, la programación y el uso de *malwares* para modificar un sistema y cambiar los resultados de una elección. Aunque la crítica se ha minimizado por las principales empresas productoras de sistemas de VPI (tal como sucedió en 2019 y 2020), en esta ocasión la propuesta de implementar el sistema generó una reacción de rechazo casi unánime (salvo, desde luego, por las empresas interesadas), ya no sólo de la comunidad académica y la de tecnología, sino también de las agencias gubernamentales relacionadas con la seguridad.

El memorándum que advertía a los Estados el "alto riesgo" de usar el VPI fue hecho por el FBI (*Federal Bureau of Investigations*), la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA por sus siglas en inglés) del Departamento de Seguridad Nacional (*Department of Homeland*

Security), la Comisión de Asistencia Electoral y el Instituto Nacional de Estándares y Tecnologías. Además, se presentaron dos informes independientes sobre el sistema de votación que se pretendía utilizar, el primero por investigadores del MIT (*Massachusetts Institute of Technology*) y el segundo por la organización *Trail of Bits*, ambas en el sentido de señalar que el sistema era vulnerable e implicaba un riesgo para la seguridad de las elecciones y para los principios constitucionales relacionados con ellas.

La experiencia comparada permite obtener dos cosas: primero, el set de principios electorales con un contenido concreto en relación a las tecnologías, que permite aterrizar la discusión sobre el VPI y tener un marco normativo claro para su análisis; segundo, nos aclara las características y particularidades técnicas de las tecnologías electorales en Internet, así como los dilemas o tensiones que tienen con los sistemas jurídicos y con su implementación empírica. Lo primero nos sirve de base para construir un modelo normativo de acuerdo al marco constitucional y legal mexicano para así evaluar el sistema de VPI del IECM (y aquellos que se propusieran después); lo segundo nos permite salir de la argumentación abstracta y declarativa sobre lo que los sistemas hacen y pueden hacer, para basarnos en hechos y evidencia técnica para criticar y evaluar el VPI.

Agrupamos los principios por su contenido en dos conjuntos: 1) por un lado, la publicidad, la transparencia y el control ciudadano; 2) por el otro, la integridad y la secrecía del voto. Los primeros corresponden a lo que el marco constitucional y legal mexicano concibe como principios centrales de las elecciones, los segundos son los elementos centrales del derecho a votar.

El primer conjunto está en tensión con la evaluación y difusión de información sobre los sistemas de VI, exige una concepción amplia de las auditorías porque si no es imposible evaluar correctamente los sistemas y demanda que todo sistema sea comprensible para las personas sin la necesidad ni la obligación de tener conocimientos técnicos especializados. La tecnología, la programación y la criptografía vuelven muy difícil lograr que la ciudadanía tenga este “control” sobre el sistema electoral, pero el

problema se agrava mucho más cuando el sistema está cerrado al análisis independiente fuera del control de las autoridades (ingeniería inversa, pruebas de penetración y recompensa y de evaluar el código abierto en su totalidad) y a la difusión e información plena de estos resultados.

El segundo conjunto (integridad-secrecía) explica cómo estos principios están en juego cuando mudamos las elecciones del espacio presencial a Internet. Sabemos ya que la tecnología implica una tensión inherente entre ambos principios que hace que las medidas que protegen a uno tiren en sentido contrario del otro, con el resultado de que por proteger la secrecía del voto sea casi imposible saber si una elección es *hackeada*. También sabemos que, por un lado, la mayoría de las auditorías centralizadas de los sistemas de VPI suelen ser incompletas o parciales y que, por el otro, en todas las experiencias internacionales en las que se permitió investigar los sistemas a través de revisiones independientes y completas, **siempre se encontraron vulnerabilidades y riesgos.**

La experiencia internacional nos da una advertencia que debemos tomar en serio: el voto por Internet tiene un doble problema de invisibilidad. Primero, porque su estudio y revisión suele hacerse de manera opaca, a manera de una "caja negra" blindada al escrutinio público (ante la falta de los códigos abiertos, la ingeniería inversa y la evaluación independiente). Segundo, porque el funcionamiento y la naturaleza de los mecanismos de seguridad de los sistemas de VPI hacen que en caso de que la elección sea *hackeada*, la manipulación del sistema y de toda la elección se vuelva invisible.

3. El caso mexicano: resultados y alarmas sobre el VPI en la CDMX

En el último apartado sistematizamos los requisitos que todo sistema de voto por Internet debería cumplir de acuerdo al marco constitucional y legal leído a la luz de los principios electorales y del voto, y de las particularidades del entorno de Internet.

El modelo responde al desarrollo internacional que puede rastrearse desde la Declaración Universal de los Derechos Humanos (DUDH), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), y la Convención Americana Sobre Derechos Humanos (CADH), hasta las decisiones de organismos especializados en la interpretación de estas normativas como lo es la Corte Interamericana de Derechos Humanos (que en este caso es de particular relevancia dado que México pertenece al Sistema Interamericano de Derechos Humanos y reconoce su autoridad en términos interpretativos sobre la CADH).

El marco internacional y regional de derechos humanos sirve de base y de puente hacia la Constitución Política de los Estados Unidos Mexicanos (CPEUM) y las decisiones jurisprudenciales en materia electoral que están relacionadas con el derecho al voto libre y secreto y a los principios centrales de las elecciones (certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad). Esquemáticamente, el modelo de los mínimos que todo sistema de VPI debe cumplir consiste en:

a) Garantizar los principios fundamentales del derecho a votar: integridad, secrecía y libertad.
    i) La integridad consiste en que el voto sea emitido como el votante decida (*cast as intended*), que sea contado como se emitió (*counted as cast*) y que pueda verificarse que el resultado de la elección corresponde a la sumatoria total de los votos emitidos por el electorado (*all votes counted as cast*).
    ii) La secrecía consiste en que ninguna persona pueda conocer la intención del voto de las y los electores aún cuando ellos quieran mostrarlo.
    iii) La libertad consiste en que las personas cuenten con las condiciones físicas y materiales para que la emisión del sufragio esté libre de coerción y de la presión de otras personas o grupos.
b) Cumplir con los principios rectores de la función electoral, en particular los de: certeza, máxima publicidad, transparencia y rendición de cuentas.

i) La certeza implica, en lo jurídico, que deben existir bases que justifiquen la adopción de un sistema de VPI y, en lo técnico, que debe haber medios suficientes para demostrar que el sistema de VPI se desarrolla como dicen que lo hace.

ii) La máxima publicidad, la transparencia y la rendición de cuentas se relacionan con los principios de publicidad y control ciudadano establecidos por el Tribunal Constitucional Alemán. Todo esto implica que primero, los pasos esenciales de la elección deben sujetarse al escrutinio público; segundo, que el público debe poder entender esos pasos y los medios con los que el voto se ejerce sin la necesidad de contar con conocimientos técnicos especiales; y tercero, que el sistema elegido para emitir el sufragio debe estar abierto al estudio independiente y experto en su totalidad, para poder evaluar todos sus componentes y asegurarse de que funcionan como las autoridades dicen que funcionan.

c) Asegurarse de que cualquier característica del sistema que pueda constituir una limitación al derecho a votar o a algún otro derecho político relacionado, cumpla con los criterios de legalidad, idoneidad, necesidad y proporcionalidad.

Los antecedentes, el marco normativo y las particularidades del VPI en la Ciudad de México

En la primera parte del análisis del voto por Internet del IECM en la CDMX, realizamos un recorrido detallado por la normatividad que sirve de marco para su establecimiento, para después explicar en qué consiste y cuáles son los avances y detalles específicos de este sistema (y delineamos algunas cuestiones problemáticas al respecto). Si bien es cierto que parte importante del sistema se sustenta en el marco legislativo y administrativo, su justificación se apoya fuertemente en algunas sentencias del Tribunal Electoral del Poder Judicial de la Federación (TEPJF), en distintas decisiones técnicas especializadas en los años en los que el VPI fue desarrollado y en las auditorías realizadas al mismo por distintas empresas, así como por la Universidad Nacional Autónoma de México (UNAM).

Por ello, estudiamos de manera detallada todas estas, en particular la sentencia hito que sirve (al menos para el IECM) de soporte para el VPI en la CDMX, emitida en el año 2012 por el TEPJF, así como las últimas auditorías que se hicieron al sistema (en el 2017 y el 2020). En este lugar tomamos también un último informe especializado hecho a pedido especial del IECM para observar y evaluar el sistema de VPI en las elecciones de Comisiones de Participación Comunitaria y la Consulta de Presupuesto Participativo 2020-2021 marzo del 2020. El informe es ilustrador porque muestra que varias de las preocupaciones presentadas en este trabajo son una realidad.

El análisis de las sentencias, las decisiones técnicas, las auditorías y el informe

La sentencia paradigmática fue resuelta en el 2012 por el TEPJF en el **SUP-JRC-306/2011.** Es muy importante entender que esta sentencia analizó un sistema de VPI anterior al que existe en la actualidad y que, por ello, no sirve para justificar el uso del sistema de VPI en la actualidad. Precisamente el hecho de tratar con tecnologías que cambian y evolucionan todo el tiempo hace que sea necesario revisarlos constantemente, por lo que aún imaginando que el análisis de la Sala Superior del TEPJF hubiera sido correcto, este fallo no puede utilizarse para legitimar el voto por Internet en General. La analizamos, sin embargo, porque el IECM la utiliza sistemáticamente para justificar el uso del VPI en el presente; literalmente, el Instituto Electoral repite una y otra vez que el TEPJF ya resolvió la cuestión del VPI al decir que el sistema (del año 2012) era seguro y confiable.

Esto es un error que debe dimensionar el uso de la sentencia. De cualquier forma, al estudiarla encontramos que tiene serios problemas sustantivos. Las y los ministros del Tribunal Electoral sostienen argumentos que ignoran por completo la forma en que funcionan los sistemas de seguridad en Internet y los riesgos inherentes de sus tecnologías, y hacen un análisis jurídico superficial que no toma en cuenta su dimensión tecnológica. El mejor ejemplo es que en distintas ocasiones, IECM y TEPJF justifican el VPI al decir que en ese tiempo era seguro realizar transacciones y operaciones bancarias por Internet, y que de eso podía deducirse que votar por Internet

también era suficientemente seguro. Por ignorancia plena o por desinterés, el TEPJF (y el IECM también, puesto que comparte explícitamente esta postura en particular) sostiene toda su sentencia en presupuestos erróneos y parciales sobre las tecnologías y la seguridad en Internet.

Al momento de la sentencia, tanto en la doctrina como en la experiencia comparada a nivel internacional, el argumento de la seguridad bancaria en Internet había sido ampliamente refutado y criticado, y existían distintas experiencias claras de los riesgos que implica usar estos sistemas. Sin embargo, no hay una sola parte de la sentencia en que esta información se tome en cuenta. En el mejor de los casos, la ignorancia (si no la mala fe) de esos hechos y estudios lleva al Tribunal a cometer errores sustantivos importantes.

En primer lugar, los magistrados nunca analizaron las complejidades inherentes a los sistemas de votación por Internet ni los riesgos informáticos, sino que simplemente refirieron a los informes realizados por el entonces IEDF y al anexo técnico presentado a éste, en donde se afirmaba que el VPI era seguro. El Tribunal debía realizar el análisis técnico de la evidencia pero sólo se conformó con hacer el análisis normativo tomando los informes como ciertos, cuando en realidad debió demostrar que los riesgos implicados no ponían en riesgo los principios constitucionales.

En segundo lugar, el Tribunal hizo un análisis incorrecto del test tripartito para evaluar si el voto por Internet era idóneo, necesario y proporcional. Contrario a los estándares interamericanos, la Sala Superior realizó un estudio superficial en el que dio por hecho cuestiones que debía demostrar. Por ejemplo, consideró que el VPI aumentaba la participación, cuando no sólo no había evidencia local sobre eso sino que a nivel internacional sí existía evidencia que apuntaba en sentido contrario (tal como mostramos en la primera parte). El Tribunal tampoco analizó si esta medida era la menos riesgosa, restrictiva o gravosa frente a otras alternativas (tal como exige el criterio de necesidad) como el voto postal. Finalmente, al analizar la proporcionalidad dio por hecho que los riesgos de estos sistemas eran mínimos y que su contribución a la participación era alta, sin detenerse a demostrar empíricamente esto o sin siquiera analizarlo sustantivamente.

El tercer problema es que tampoco analizaron ninguno de los otros posibles riesgos de estos sistemas, como son los relativos a los usuarios, la posibilidad de la coerción o el uso de *malware* para infectar los dispositivos. Por el contrario, la Sala Superior consideró que esos riesgos eran "responsabilidad exclusiva del ciudadano", mostrando nuevamente su ignorancia sobre el tema. Un punto muy ilustrativo sobre los problemas de la interpretación del Tribunal es que para justificar su decisión, se ampararon en las reglas de la experiencia y la lógica, a través de las que consideraron que era claro que no había riesgos y que tenía sentido comparar de manera análoga el VPI con la banca por Internet. El punto es claro porque es imposible entender los riesgos y particularidades del voto por Internet desde ahí y, por el contrario, requiere de un conocimiento especializado relacionado con la ciencia computacional y la tecnología.

Posteriormente hubo dos sentencias del Tribunal Electoral del Distrito Federal que continuaron la tendencia de la decisión de la sala superior: TEDF-JEL-017/2013 y TEDF-JEL-045/2016. En ambos casos se repitió el patrón iniciado por la Sala Superior, tanto en su forma de analizar los casos como en sostener ciertos presupuestos sin respaldo empírico, como el del aumento de la participación, donde (en la primera sentencia) el Tribunal consideró que era "indudable" que este tipo de sistemas fomentaba el interés y aumentaba la participación.

El análisis de **los informes del Comité Técnico del Instituto Electoral del Distrito Federal** permite acercarnos por primera vez a la forma en que son hechas las revisiones a los sistemas de VPI en México. Dos cosas significativas son, primero, el señalamiento de que al parecer el Comité sólo revisó algunas etapas del sistema y que el enfoque de esas revisiones fue sobre **su usabilidad y funcionalidad,** más que sobre la seguridad y, segundo, el señalamiento de que "no se hicieron revisiones a aspectos más profundos de su constitución". También es ilustrativo sobre el tema de la transparencia, ya que la información pública permite ver que el Comité hizo una recomendación técnica consistente en el "Fortalecimiento de Aplicación de Estándares de Seguridad", sin que esa información esté disponible. Como se muestra en el caso de las auditorías, esto es común puesto que es parte

de una práctica cotidiana de que los hallazgos de seguridad no son hechos públicos y son generalmente comunicados sólo a las unidades técnicas del Instituto.

Las auditorías son, junto con el informe externo final, la forma más fiable y cercana de conocer el funcionamiento y las cuestiones de seguridad del sistema de VPI del IECM, dado que no están habilitadas las pruebas de penetración y recompensa ni los estudios independientes y dado que el código no es abierto salvo a las instituciones elegidas por el propio Instituto para auditar el sistema. En este caso, las auditorías analizadas se realizaron en el 2017 y el 2020 respectivamente. En el 2017 las auditorías fueron hechas por una empresa (Grupo Scanda-Kimat) y por la UNAM (un área especializada de la Facultad de Estudios Superiores -FES- Aragón), y en el 2020 nuevamente por la UNAM y además se contó con el informe externo encargado a dos investigadores extranjeros.

En todos los informes hay afirmaciones que son preocupantes de las que no se puede saber más detalles porque la información específica de la que derivan no es pública. En el caso de la auditoría de la empresa Kimat en el 2017, por ejemplo, señalan que el tiempo que tuvieron para realizar las pruebas fue corto, que encontraron fallas de seguridad en el cifrado (y recomendaban que fuera más robusto), que había riesgos de interferencias de terceros en el sistema de votación, que era necesario tomar en cuenta "puntos de mejora" y que el sistema tenía un nivel "razonable" y "aceptable" de seguridad y confianza.

La primera auditoría de la UNAM (2017) refleja el problema de opacidad señalado anteriormente: de manera explícita, reconoce que se "obtuvieron hallazgos" de seguridad que fueron comunicados en un "reporte técnico" al IECM de manera privada. También señalaron que podían haber obtenido mejores resultados de contar con mayor tiempo y que no pudieron estudiar con la profundidad ideal el análisis interno de seguridad, por lo que obtuvieron resultados menores de los que podían haber logrado. En esta primera auditoría es claro que el enfoque de las auditorías se ha realizado sobre su usabilidad y funcionalidad y no sobre la seguridad desde una perspectiva integral que evalúe los distintos tipos de atacantes posibles y las formas en que una elección puede ser manipulada.

La segunda auditoría de la UNAM (2020) es similar en muchos sentidos. Primero porque los hallazgos de errores y de riesgos de seguridad tampoco son públicos y se entregaron a la Unidad Técnica de Servicios Informáticos del IECM, pero no están abiertos al escrutinio público. La auditoría encontró errores de distintos grados y concluyó que los dispositivos eran "**aceptables** en materia de seguridad", sin explicar en qué consistían los errores y los riesgos. En el análisis del código se encontraron 53 vulnerabilidades y al menos una de carácter crítico, dando en algunos aspectos la peor calificación por hallazgos en el código. Sin embargo la conclusión de la UNAM fue que el sistema era seguro y hacía lo que debía hacer y nada más. Es interesante señalar esta auditoría porque, al contrario de lo que señaló, **el sistema de VPI del IECM falló en las elecciones de marzo de 2020** e impidió que muchas personas pudieran ejercer su derecho al voto.

El sistema falló y **el informe externo final, pedido por el propio IECM,** es categórico al señalar que el sistema de VPI funcionó con distintos riesgos que no fueron tomados en cuenta por las autoridades, tales como la posibilidad del robo de credenciales de los usuarios, el uso de *malware* para robar el voto, problemas del sistema que podían llevar a romper el proceso de anonimización en caso de *hackear* la elección y otra serie de riesgos relacionados con partes del sistema que no fueron auditados y otros que se corrieron en las jornadas electorales. También es contundente al señalar que las auditorías realizadas por la UNAM tienen un enfoque de funcionalidad y usabilidad y que no profundizan lo suficiente en elementos fundamentales del sistema como el *software*, la información sensible y el análisis desde una perspectiva de seguridad que tome en cuenta los diversos tipos de atacantes y los escenarios de riesgo de una elección (y que son fundamentales para evaluar realmente la seguridad de un sistema de VPI).

Por estas razones subrayan, entre otras cosas preocupantes, que: i) el proceso de estimación de riesgos del sistema no es exhaustivo ni tiene el enfoque correcto de seguridad que requiere; ii) la tecnología tiene el problema inherente de la tensión secrecía-integridad, lo que hace que sea posible el uso de *malwares* que afecten los votos antes de que sean cifrados; iii) este problema inherente vuelve imposible la verificabilidad del sentido

del voto y las posibles soluciones escapan a la comprensión de todos los ciudadanos (por su complejidad tecnológica); y iv) que las auditorías tienen problemas serios de transparencia y publicidad, por la imposibilidad de contar con la información pública más importante sobre los hallazgos de esas mismas auditorías.

Lo anterior lleva a varias conclusiones que deben ser una alerta sobre el VPI: primero, que los análisis realizados al sistema han sido limitados y se han desarrollado bajo una lógica de "seguridad por oscuridad" (*security by obscurity*) debido a las limitaciones y a que no existe la posibilidad de realizar revisiones independientes que puedan conocer la totalidad del código del *software* y hacer ingeniería inversa y pruebas de penetración y recompensa; segundo, que la conclusión sobre la funcionalidad del VPI hechas por la auditoría de la UNAM "se reveló falsa durante la jornada" ante el hecho de la falla del sistema; y tercero, que todos estos problemas tuvieron como "consecuencia directa la privación del ejercicio del voto para muchos ciudadanos".

CONCLUSIONES

A lo largo de este trabajo evaluamos de la manera más completa posible la alternativa del voto por Internet. Los argumentos, las experiencias y el modelo democrático arrojan advertencias para ser leídas en un mismo sentido: no es posible hoy en día y muy probablemente tampoco lo será en el futuro, que el voto por Internet logre garantizar los principios democráticos del voto y de las elecciones.

La defensa del voto por Internet se sustenta en argumentos que se presumen verdaderos a priori pero que no se sostienen cuando los evaluamos en la realidad. El elemento de su seguridad tal vez sea el mejor ejemplo de todos: los defensores de esta modalidad señalan una y otra vez que se trata de un sistema seguro y lo asocian al ejemplo de la banca y las compras por Internet, cuando el ámbito electoral y el bancario-comercial son estructuralmente distintos. Las reglas que hacen funcionar a uno son inaceptables e incompatibles para el otro.

El intento de adaptar la tecnología a las votaciones lleva a un problema inherente del voto por Internet que tiene en su centro una tensión inevitable e irresoluble entre la secrecía del voto y la integridad de las elecciones (y del voto mismo). No hay forma de escaparle sin sacrificar un principio por el otro. Las medidas que sin duda deberían tomarse para proteger la secrecía del voto por Internet hacen que sea imposible verificar su integridad y las medidas que sin duda deberían tomarse para proteger la integridad vulneran la secrecía, por más que sus defensores intenten obviar esta realidad.

El voto por Internet en la actualidad es incapaz de lograr el grado de transparencia y de publicidad necesarios para las sociedades democráticas; su funcionamiento cerrado, la revisión superficial y la imposibilidad del control ciudadano lo vuelven un sistema que en lugar de regirse por el escrutinio público y el entendimiento ciudadano se rige por la fe en los sistemas y las tecnologías. Ver, saber y entender lo que pasa en las votaciones es indispensable para lograr la legitimidad democrática, tanto de las elecciones como de los gobiernos que resultan electos de ellas. Optar por esta opción implica que creamos en algo que no podemos ver y que tampoco podemos entender como funciona.

El sistema del Instituto Electoral de la Ciudad de México no cumple con prácticamente ninguno de los elementos mínimos que un sistema de votación debería tener, se sostiene en varios supuestos equivocados y funciona de acuerdo a prácticas e ideas que ponen en riesgo (y han efectivamente violentado) el derecho a votar de las y los ciudadanos mexicanos en la Ciudad de México y en el extranjero. En el contexto mexicano, donde la coerción, la violencia, la desigualdad y el riesgo de fraudes electorales son problemas reales y permanentes, todos estos problemas y riesgos no hacen más que profundizarse.

¿Qué aprendizajes nos deja este estudio para las futuras discusiones sobre el voto por Internet (tanto a nivel local como nacional)? Primero, que el enfoque general de las autoridades suele minimizar la dimensión técnica y tecnológica del voto por Internet. De no ser así, las autoridades no podrían sostener que un sistema en Internet garantiza la “certeza absoluta” que exige la legislación. Esto es simplemente falso en términos empíricos.

Segundo, que la revisión y auditorías a los sistemas de voto por Internet en la experiencia mexicana son, como mínimo, insuficientes. El enfoque de la revisión ha sido 94 más de corte funcional que de riesgo crítico, dando mayor peso a las cuestiones de flujo, operación y continuidad, y con un menor énfasis en las cuestiones de los riesgos del *software,* la información sensible y los riesgos no sólo de los servidores sino de los usuarios (que hasta la fecha, no han sido siquiera considerados ni mencionados por ninguna auditoría pública o privada en México). Las auditorías se han estandarizado sin tomar en cuenta cuestiones particulares relevantes para evaluar la seguridad, tales como el tipo de atacante, su poder relativo de penetración, escenarios de ataques estatales, etc. No es para nada claro que las auditorías hayan sido suficientes para evaluar el sistema de voto por Internet de la Ciudad de México y, más bien, hay dudas serias de que su enfoque pueda probar que el sistema es tan seguro como nos dicen que es.

Tercero, que la ciudadanía ha transitado la historia del voto por Internet sabiendo sólo una parte de la historia: la versión de las autoridades electorales. Durante años, ha existido en las auditorías información reservada sobre los hallazgos en materia de seguridad, que no se hace pública y queda solamente en manos de los funcionarios (y a veces sólo en las de los técnicos) del Instituto. Esto no sólo viola el derecho de acceso a la información pública reconocido por la Constitución, sino que afecta fuertemente a los principios electorales de la máxima publicidad, la transparencia y la certeza. El discurso del voto por Internet se ha construido, en este sentido, sobre una lógica de *security by obscurity* (seguridad por oscuridad) que deja fuera del escrutinio público información importantísima.

Cuarto, que los problemas de auditorías y transparencia nos permiten generar exigencias concretas tanto para las y los legisladores como para las autoridades electorales: 1) el voto por Internet debe ser abandonado por los riesgos que implica para la legitimidad política de las elecciones pero, en caso de no ser así: 2) es indispensable contar con auditorías independientes en el sentido amplio que se reconoce en la experiencia internacional, que incluyen pruebas de penetración y recompensa, realización de ingeniería inversa para probar la seguridad y la participación de expertos

internacionales especializados en el tema; 3) la información técnica que se reserva en las auditorías para entregarse a las unidades técnicas debe ser pública porque es el núcleo que permite evaluar la gravedad de los hallazgos de seguridad y funcionalidad de los sistemas; 4) en cumplimiento con su deber de transparencia e imparcialidad, las autoridades deben socializar de manera completa la realidad compleja del voto por Internet; las cosas que están en juego y los riesgos, y no solamente su cara buena y optimista. No se trata de una cuestión de opiniones sobre si el voto por Internet nos gusta o no, se trata de hechos, datos e información técnica que debe ser socializada para que la ciudadanía evalúe por sí misma el riesgo o seguridad del voto por Internet. Es profundamente antidemocrático dejar cierta información fuera y confiar en la palabra, que puede ser parcial o no (imprecisa o no, incompleta o no), de los entes que participan en la implementación del sistema.

La fe ciega en algo que no podemos entender puede ser razonable e incluso admirable cuando se trata de asuntos de religión, pero cuando tratamos asuntos terrenales, en los que el poder político y la democracia están en juego, renunciar al escrutinio público y a los controles democráticos es simplemente un error. Las elecciones no son, y no deberían de ser nunca, un asunto de fe.

R3D

Red en Defensa
de los Derechos Digitales

@R3D