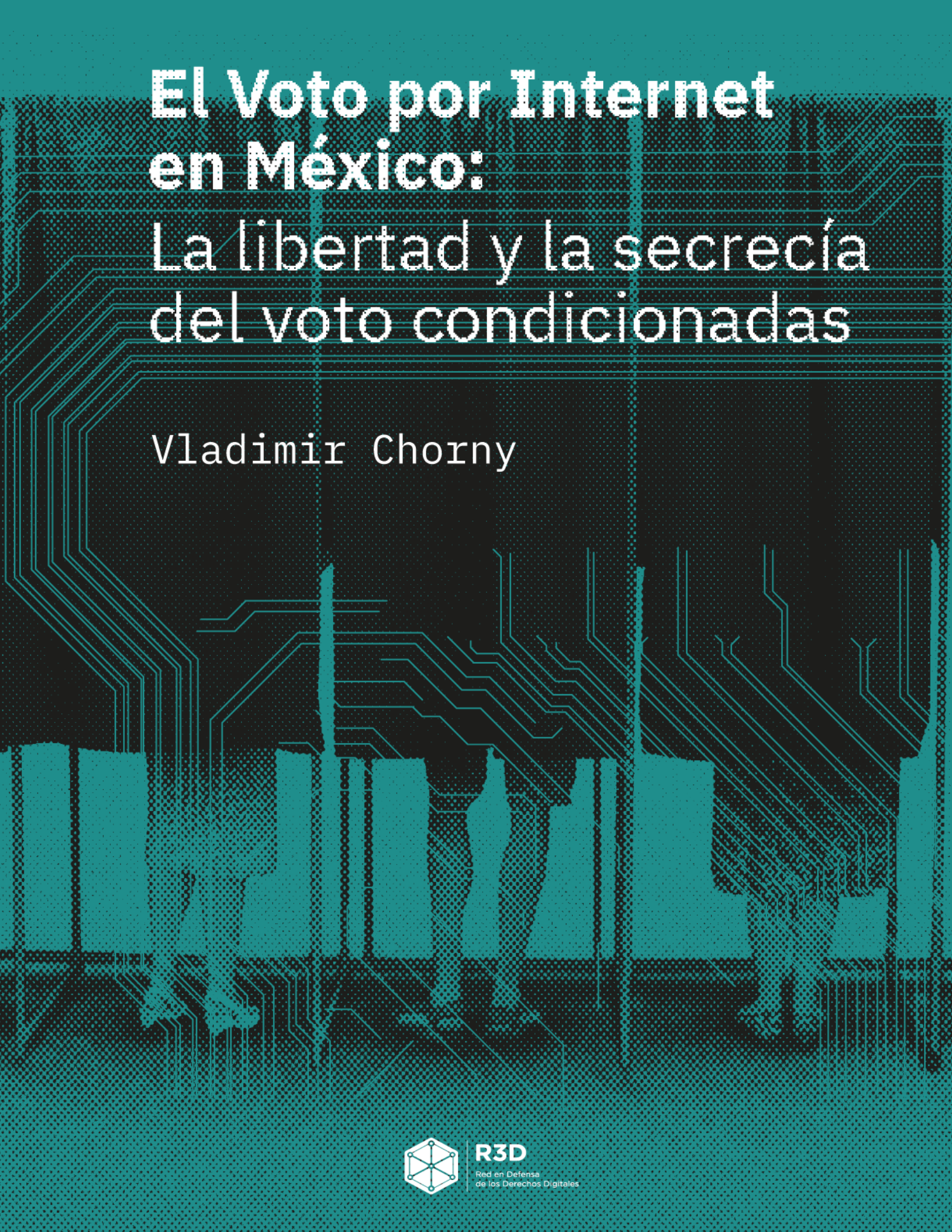
El Voto por Internet en México:
La libertad y la secrecía del voto condicionadas

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.

DISEÑO EDITORIAL: **FÓSFORO**

Ciudad de México. México, octubre 2020

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

Índice

"Cuando emita la boleta a través del sistema de entrega segura online, usted está renunciando voluntariamente a su derecho al voto secreto y asumiendo el riesgo de que ocurra una transmisión incorrecta"

- Aviso de no responsabilidad (*Disclaimer*) del sistema de voto por Internet en Alaska[1]

1. Fitzgerald, Caitriona; Smith, Pamela; Goodman, Susannah. *The Secret Ballot at Risk: Recommendations for Protecting Democracy, Electronic Privacy Information Center, Verified Voting and Common Cause*, August 18, 2016, p. 3. Disponible en: https://www.secretballotatrisk.org/Secret-Ballot-At-Risk.pdf.

Vivimos en sociedades interconectadas donde cotidianamente realizamos actividades importantes de nuestras vidas a través de Internet (operaciones bancarias, compras de artículos y pago de servicios, registro de nuestros estudios médicos, etc.). Tanto Internet como las tecnologías han abierto un camino para el ejercicio de los derechos (educación, cultura, acceso a la información, libertad de expresión, etc.) en el mundo digital y, en esta dirección, algunas personas y autoridades consideran la idea de votar por Internet como el siguiente paso en la modernización y el desarrollo de las democracias. Votar sin la necesidad de los cuerpos presentes, a través de un celular o una computadora (por medio de una aplicación especial), se plantea hoy casi como una panacea para fortalecer uno de los pilares de las democracias modernas: el derecho al voto universal, libre y secreto.

¿Qué tanto de la promesa del Voto por Internet (en adelante VPI) es cierta? ¿La modalidad virtual del sufragio es capaz de garantizar sus principios fundamentales? ¿Qué tan seguro es votar por Internet? ¿Las tecnologías son suficientes para proteger las elecciones? ¿Cuáles riesgos enfrentan los sistemas (el *software*) y los dispositivos (el *hardware*) y cómo se han resuelto? ¿Se han resuelto? ¿Es posible garantizar el voto libre y secreto en Internet y dotar de legitimidad política a las elecciones en el mundo digital?

Nuestro estudio busca responder estas preguntas al analizar detalladamente las dimensiones más importantes del voto por Internet. Por un lado, nos interesa mostrar cuáles son los **problemas empíricos y técnicos** que tienen los sistemas de VPI (Parte I). Por otro lado, queremos analizar los **elementos normativos** del derecho al voto y los principios rectores de las elecciones a partir de tres casos paradigmáticos relacionados al VPI: Alemania, Estonia y los Estados Unidos de América (Parte II). Finalmente, proponemos un modelo normativo a partir de los estándares internacionales de derechos humanos y el marco constitucional mexicano que toma en cuenta las particularidades técnicas y científicas de las tecnologías relacionadas con el voto por Internet, para revisar el caso más avanzado de este fenómeno en México: el Sistema Electrónico por Internet (SEI) del Instituto Electoral de la Ciudad de México (IECM) (Parte III).

PARTE I / El Voto por Internet y su dimensión técnica y empírica

1. Argumentos a favor y en contra del Voto por Internet

La modernización y el optimismo sobre las nuevas tecnologías suelen ser la base de los partidarios del voto por Internet. A partir de ahí se desarrollan argumentos que lo plantean como una práctica revolucionaria frente a las limitaciones de las otras alternativas de votación (presencial o postal). Aunque intuitivamente pensemos en los gobiernos cuando imaginamos las elecciones en las sociedades democráticas, en el caso del Voto por Internet uno de los sujetos principalmente interesados en su despliegue son las empresas que desarrollan la tecnología o que facilitan el *software* para llevar a cabo las elecciones, por lo que algunos argumentos son de carácter técnico y no meramente político o normativo.[2]

Sin embargo, no todas las cosas que se dicen del VPI son precisas y algunas otras, más que imprecisas, son infundadas o erróneas (tanto en términos técnicos como político-jurídicos). Al menos durante las últimas dos décadas, investigadoras e investigadores especializados en tecnología y en ciencia computacional en distintos lugares del mundo han dedicado su trabajo a analizar el funcionamiento de los sistemas de voto electrónico en general y de los sistemas de voto por Internet en particular.[3] A partir de la evidencia empírica y el análisis teórico podemos responder qué es cierto y qué no sobre el tema. A continuación desarrollamos punto por punto cuáles son los problemas que pueden plantearse frente a los supuestos beneficios del VPI.

2. Para ver un ejemplo de la estructura y la comunicación de una empresa de VPI al respecto, ver: "Scytl, Beneficios del voto por Internet" en: https://www.scytl.com/es/online-voting-benefits/.

3. Debemos aclarar que en este trabajo no estudiamos la modalidad del Voto Electrónico (VE), aunque hay elementos de éste que son relevantes para pensar y evaluar el VPI. El voto electrónico puede tener distintas modalidades como la boleta única electrónica que imprime un registro de papel (que contiene un chip) (u otros que no emiten el papel). Es un mecanismo que combina normalmente una máquina donde las personas llegan a votar como lo harían en otra casilla, sólo que las boletas son electrónicas y no se utilizan las tradicionales de papel. El voto por Internet no requiere la presencia de la persona que vota, ya que puede hacerlo de manera remota a través de una *app* (aunque también puede habilitarse un lugar de votación donde la persona se puede acercar para votar ahí por medio de la *app*), como explicamos más abajo. El VPI permite que una persona vote a través de un *click*, sin que exista ningún respaldo en papel.

A. ¿El VPI aumenta la participación política?

El argumento más común a favor del VPI es que es fundamental para aumentar la participación política y hacer que la gente vote más. Supuestamente, la tecnología potencia la participación política porque quita de en medio los obstáculos de acceso y tiempo que las personas enfrentan al votar (distancias, clima, tiempo de espera, etc.). En otras palabras, hace menos exigente la participación y esto hace que aumente. La idea es común al hablar del voto en el extranjero, ya que se considera que el VPI "remueve las fronteras" y facilita la participación de las personas que se encuentran lejos.

El argumento debe demostrarse empíricamente más allá de que sus premisas nos parezcan intuitivas. Pero para hacer este análisis primero debemos despejar algunas cuestiones metodológicas sobre la participación política, en especial porque como mostramos en seguida, el argumento se sostiene en supuestos que se dan por hecho pero que no necesariamente son ciertos. Lo que queremos decir es que las afirmaciones de este tipo deben demostrarse, no presumirse (deben ser una conclusión y no un punto de partida), aunque esto muy pocas veces es así.

Estrictamente hablando, el hecho de que sea más fácil votar usando una *app* (suponiendo que esto fuera así), no nos lleva directamente a la conclusión de que más gente va a elegir votar por ese medio. Si, por ejemplo, las personas desconfían de un sistema de Internet, probablemente no lo usen aún si les facilita votar. Lo mismo si el sistema falla o la plataforma es complicada de usar. La confiabilidad, la usabilidad y otros factores impactan en el hecho de que las personas utilicen o no un sistema de votación, y eso significa que el argumento no se sostiene por sí mismo.[4]

Hay además otros factores que problematizan el argumento de la participación. Variables contextuales importantes tales como la desigualdad estructural de un país (los números de pobreza y de falta de acceso a tecnología necesaria para usar el sistema), el grado de brecha digital (qué tantas personas entienden la tecnología y están capacitados para utilizarla en ejercicios como éste) y el nivel de confianza en las instituciones que se

4. Las preocupaciones sobre la seguridad del sistema pueden combinarse con las dudas de la integridad de un proceso electoral, poniendo en riesgo la legitimidad de una elección y afectando incluso la participación política por dar la impresión de que ir a votar en esas condiciones no hace ninguna diferencia. Germann, Micha y Serdült, Uwe. "Internet voting and turnout: Evidence from Switzerland", *Electoral Studies*, Vol. 47, June 2017, pp. 3-4.

encargan del ejercicio electoral son todas puntos que inevitablemente pueden jugar en contra de la aceptación y el uso del sistema y son relevantes para evaluar este argumento.

Estudios empíricos señalan, por ejemplo, que la participación política no aumenta significativamente comparada con otras alternativas como el voto postal (por correo), en particular cuando este último se acompaña de políticas públicas como el registro automático de ciudadanos (en parte porque la gente considera que esta modalidad no implica riesgos como el *hackeo* de la elección por Internet). De hecho, a nivel internacional no hay experiencia contundente que demuestre el aumento de participación por el VPI en todos los casos, sino que la evidencia apunta en distintas direcciones (muchas de ellas poco alentadoras), con varios estudios empíricos que muestran lo contrario.[5]

La experiencia de Suiza es un caso contundente en contra. En un conocido estudio que analizó las votaciones en Ginebra desde el 2003 hasta el 2017 y en Zurich del 2005 al 2011, en un contexto en el que el VPI compitió frente al voto postal durante años en numerosas elecciones, se llegó a la conclusión de que el VPI no aumentó la participación política ni tuvo mejores resultados que el voto postal.[6] En distintos estudios, detallados para evaluar la causalidad "VPI-participación", los investigadores descubrieron que no existía tal. El VPI no aumentaba la participación política ni era mejor que el postal en este sentido. [7]

El aumento de la participación debe entonces medirse tomando en cuenta estos factores (es multicausal). Sin embargo, muchas veces el argumento se defiende con encuestas o inferencias de preferencias de las personas, cuando no existe experiencia previa con la que se pueda

5. Un gran ejemplo al respecto es el del caso de Estonia (que desarrollamos con detenimiento más adelante) donde, mientras que unos señalan que en las votaciones locales del 2009 el VPI aumentó en 2.6% la participación, otros muestran que en las elecciones nacionales del 2007 esto no fue así. Sobre el primer punto ver: Trechsel, Alexander; Vassil, Kristjan. Internet Voting in Estonia: a Comparative Analysis of Four Elections since 2005, Report for the Council of Europe, 2010. Para el segundo punto ver: Bochsler, Daniel. "Can Internet voting increase political Participation? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections", Paper Prepared for Presentation at the 'Internet and Voting' Conference. Fiesola, June, 2010.

6. Es importante mencionar que debido a dudas de seguridad y preocupaciones jurídicas por la manipulación de elecciones, tanto en Ginebra como en Zurich las votaciones por Internet fueron suspendidas o descontinuadas en distintas ocasiones (la primera entre 2005 y 2008, la segunda en 2011, retomando en 2015 pero sólo para ciudadanas en el extranjero). Germann, Micha y Serdült, Uwe. "Internet voting and turnout..." *op. cit*. pp. 3-4.

7. *Ibidem,* p. 2; Archer, Keith, *et. al. Recommendations Report to the Legislative Assembly of British Columbia,* Independent Panel on Internet Voting, February 2014, p. 12.

contrastar o cuando las personas no cuentan con información completa. Las metodologías cuestionables deben refutar estudios completos como el de Suiza, que muestran que la gran mayoría de personas que tuvieron la posibilidad de votar por Internet prefirieron hacerlo por la vía postal. [8]Precisamente en este sentido:

> "... el voto postal frecuentemente genera menos preocupaciones de seguridad [...], las preocupaciones sobre la seguridad del voto online pueden balancear los beneficios potenciales de su conveniencia o, en casos extremos, incluso disminuir la participación general. Además, el voto postal se extiende a una audiencia mayor porque no presupone ni el acceso a Internet ni las habilidades necesarias sobre las tecnologías. Esto podría significar que el voto postal supera al voto por internet en términos de incrementar la participación".[9]

Suponiendo que el argumento a favor del VPI y la participación política fuera cierto, aún faltaría responder la cuestión de si el aumento (que en la gran mayoría de experiencias, de haberlo, es poco significativo) justifica el uso de una tecnología que puede tener otros serios problemas, como el de ser inseguro o el de que ponga en juego la secrecía del voto (tal como explicamos más abajo).

Si miramos la experiencia de la Ciudad de México sobre el VPI, es muy interesante ver la comparación de los ejercicios sobre el voto en el extranjero y de las consultas participativas desde el momento en que se instauraron (2011-2012) hasta ahora, con especial atención en lo que sucedió con las elecciones para la Jefatura de Gobierno de la CDMX frente a la opción del voto postal.

En el año 2012, tanto el voto postal como el VPI estuvieron habilitados para el voto en el extranjero, por lo que existieron dos Listas Nominales distintas correspondientes a cada elección. El total de votantes de ambas modalidades de votación fue de 7,915 electoras y electores (y la suma las dos Listas Nominales 10,782), cuya distribución se dio de la siguiente manera: para la **votación postal**, se registraron 6,592 ciudadanos en la Lista Nominal y votaron 5,276 (80.04%); para la **votación por Internet**, se registraron en la Lista Nominal 4,190 ciudadanas y votaron 2,639 (62.98%). [10]

8. Otro dato interesante del VPI en Suiza es que está limitado a un máximo de 30% de personas que pueden realizarlo dentro de cada cantón, precisamente para mitigar los riesgos frente a la elección en casos de que el sistema sea manipulado. Germann, Micha y Serdült, *op. cit.*, p. 4.
9. *Ibidem*, p. 11.
10. Información Estadística de los Resultados 2012, IECM, disponible en: http://secure.iedf.org.mx/resultados2012/voto-extranjero.php?ve=1.

En el año 2018, la elección a la Jefatura de Gobierno no tuvo habilitada la modalidad de VPI pero la participación electoral en el extranjero para esta elección aumentó considerablemente: frente a los 10,782 ciudadanos y ciudadanas inscritos en las Listas Nominales en el 2012, se inscribieron 28,803 votantes, de los que votaron 20,839, (72.35%), la más alta en la historia de las últimas dos décadas de la capital del país.

Aunque el VPI no se utilizó para la elección a la Jefatura de Gobierno en el 2018, sí continuó utilizándose para el ejercicio de Consulta Ciudadana sobre Presupuesto Participativo. Desde el año 2013 (con referencia a información del 2012) la información oficial presentada por el IECM muestra los siguientes datos:

- Consulta Ciudadana sobre Presupuesto Participativo 2013 (año 2012); Total de opiniones emitidas 144,895; **Opiniones emitidas por el SEI 15,513;** Porcentaje 10.70%.
- Consulta Ciudadana sobre Presupuesto Participativo 2014 (año 2013); Total de opiniones emitidas 876,910; **Opiniones emitidas por el SEI 137,231;** Porcentaje 15.65%.
- Consulta Ciudadana sobre Presupuesto Participativo 2015 (año 2014); Total de opiniones emitidas 188,807; **Opiniones emitidas por el SEI 37,045;** Porcentaje 19.62%.
- Consulta Ciudadana sobre Presupuesto Participativo 2016 (año 2015); Total de opiniones emitidas 276,054; **Opiniones emitidas por el SEI 98,195;** Porcentaje 35.57%.
- Consulta Ciudadana sobre Presupuesto Participativo 2017 (año 2016); Total de opiniones emitidas 764,589; **Opiniones emitidas por el SEI 58,357;** Porcentaje 7.63%. Sin embargo, en este caso importa destacar que del porcentaje total, **solamente el 1.41% votó de manera remota,** mientras que el 6.22 lo hizo en los módulos de opinión instalados por el IECM[11].
- Consulta Ciudadana sobre Presupuesto Participativo 2018 (año 2017); Total de opiniones emitidas 290 614; **Opiniones emitidas por el SEI 4 589;** Porcentaje 1.58%. Esta elección presenta el porcentaje más bajo de todos, decreciendo 95.33% frente al año 2016.[12]

La información nos permite ver que, particularmente en los últimos dos ejercicios participativos, hay un decremento muy importante en el uso del

11. IECM. Estadística de Resultados. Elección de comités ciudadanos y consejos de los pueblos 2016. Consulta ciudadana sobre presupuesto participativo 2017, Tomo II, 2017, p. 9. Disponible en: http://portal.iedf.org.mx/biblioteca/descargasC.php?id=323.
12. IECM. "Estadística de resultados de la Consulta ciudadana sobre presupuesto participativo 2018", IECM, septiembre de 2018. Disponible en: http://portal.iedf.org.mx/biblioteca/descargasC.php?id=354.

sistema pero, más aún, que parece claro que cuando se trata de votar de manera remota (utilizando los dispositivos desde el hogar u otro lugar fuera de los espacios instalados por la autoridad electoral), el porcentaje disminuye dramáticamente (sólo el 1.41% y el 1.58% del total de los votos de cada elección) porque las personas prefieren ir a votar presencialmente en los módulos presenciales del SEI.

Cuando analicemos el caso concreto del VPI en la Ciudad de México (Parte III de este trabajo) veremos que el último ejercicio realizado en el 2020 apunta en una dirección desfavorable para el argumento de la participación y que, incluso, las fallas en el sistema hicieron que muchas personas perdieran la posibilidad de votar y no pudieran ejercer su derecho a participar.

B. ¿Es una herramienta que hace el voto más accesible, cómodo y práctico?

Un segundo argumento relacionado con el de la participación es que votar desde casa o el lugar que cada persona elige, utilizando su dispositivo conectado a Internet vuelve al voto más cómodo, práctico y accesible (además de ayudar a resolver situaciones de personas que, sea por discapacidades o por una situación geográfica, tienen dificultades para ir a la casilla de votación). Las personas pueden, dice el argumento, votar desde la comodidad de sus casas sin tener que salir de ellas o sin siquiera levantarse de un sillón, sólo necesitan un teléfono inteligente o una computadora para votar sin ningún esfuerzo.

La realidad es que los sistemas de voto por Internet varían mucho en su complejidad, según el diseño del *software* de cada aplicación por la que se realiza el proceso de votación y también de acuerdo a las capacidades técnicas de cada sistema en concreto. A grandes rasgos, los sistemas de VPI funcionan de la siguiente manera:

Primero hay un proceso de autentificación de la persona votante por medio del uso de contraseñas, credenciales u otros medios que se realizan en la plataforma o aplicación con la que se va a votar. Normalmente suele haber una etapa de pre-registro en la que la persona manifiesta su intención de realizar el voto por esta modalidad y da sus datos para que se almacenen hasta el día o días de la jornada electoral.

Cuando llega el momento de la jornada electoral, la persona ingresa en la aplicación y presenta el documento y/o contraseña para autentificarse y poder ejercer su derecho a votar. La persona vota y su voto se encripta en el dispositivo, lo que supone que el fraude o manipulación durante la transmisión y recepción del servidor no es posible. Los votos cifrados se firman digitalmente en el dispositivo del votante con claves de itinerancia que aseguran la elegibilidad del votante y la protección de la integridad del voto. La mayoría de los sistemas tienen un elemento llamado "recorded-as-cast" que da un recibo electrónico al votante sobre la emisión y almacenamiento de su voto, que se registra luego también en un tablón público donde están los votos emitidos.

Luego los servidores verifican que el contenido de los votos codificados es válido sin descifrarlos, para separar los votos válidos de los no válidos. Los votos son posteriormente descifrados por un sistema que primero separa el sentido del voto de la identidad de la persona, y luego los junta de forma aleatoria para proteger el anonimato del votante cuando se descifra el contenido de su voto (esto se logra con un proceso llamado "mixing", en el que los votos se alternan o se "barajan" digitalmente y la correlación entre voto encriptado y votante se rompe). La integridad final de las urnas es verificada por sistemas matemáticos y de comprobación en donde se hace una comparación entre votos y votantes, dependiendo de las particularidades del sistema.[13]

¿Qué tan simple es votar en un sistema de este tipo? La respuesta es que "depende". De manera similar al argumento de la participación, el argumento de la comodidad tiene presupuestos "habilitantes" que deben analizarse en los hechos para ver si efectivamente es o no más accesible, cómodo y práctico. La desigualdad económica y la brecha digital son dos realidades de muchos países desiguales que van en contra de esos supuestos habilitantes. Parece demasiado obvio para señalarlo pero en el fondo no lo es: quien no tiene un teléfono inteligente o una computadora no puede usarlos para votar por Internet; quien no sabe usarlos aún teniéndolos (o debe hacer un gran esfuerzo para lograrlo porque no entiende la tecnología) tampoco. Ambos problemas funcionan como contra-argumento en este

13. Para una muestra detallada sobre los pasos y formas en que funciona uno de los sistemas de voto por Internet (el de Scytl), ver: https://www.scytl.com/es/seguridad-tecnologia-voto-internet/; y https://www.scytl.com/en/resource/secure-fully-verifiability-online-voting/.

punto, particularmente en los países donde la desigualdad y el analfabetismo digital están profundizados (tal como sucede en el caso de México).

No es lo mismo pensar la comodidad de usar el VPI en abstracto que en concreto. ¿Es igual de cómodo y práctico el sistema de VPI para las y los jóvenes que son nativos digitales (y les puede parecer novedoso), que para los adultos mayores que -en el mejor de los casos- utilizan sus teléfonos inteligentes con menos experticia que la juventud? ¿Es igual de accesible una aplicación cuando es utilizada por una persona acostumbrada a la tecnología que cuando la utiliza una persona que sólo usa su teléfono para navegar por redes sociales o comunicarse con sus familiares?[14]

La mayoría de los países que usan el VPI no tienen estudios empíricos desagregados por sujetos y grupos, que analicen estas preguntas a la luz de categorías como el género, la edad, la clase social o el grado de educación de las personas votantes. No se trata de una cuestión esencializada o estigmatizante, porque la tecnología puede ser usada y comprendida tanto por alguien con educación universitaria como por alguien no escolarizado, sino de entender la forma en que la desigualdad y la falta de educación (en este caso digital) afectan a los distintos grupos de forma diferenciada. Más adelante mostramos que, en general, todos los sistemas de VPI tienen dificultades de uso y particularidades que pueden volverlos poco prácticos o exigir un esfuerzo considerable para usarlos, poniendo en entredicho el argumento del acceso, la comodidad y la practicabilidad.

C. ¿Es seguro?

Todos los sistemas de VPI sostienen que se apegan a los más altos estándares de seguridad informática-tecnológica y que garantizan la seguridad total de las elecciones. Algunos se animan un poco más y afirman incluso que pueden garantizar certeza total de que el sistema es seguro. En general, el VPI cuenta con mecanismos de seguridad y verificabilidad de extremo a extremo, a través de protocolos criptográficos avanzados que buscan garantizar el anonimato y la privacidad. Supuestamente, tanto los datos de las personas como el sentido de su voto se mantienen secretos y protegidos, y

14. Desde luego que esto no significa que los adultos mayores no utilicen Internet o no puedan hacerlo, sino que ese hecho debe analizarse de manera situada, tomando en serio las diferencias entre los posibles grupos que utilizan el sistema. La relación edad-comodidad toma relevancia en especial cuando la pensamos desde el problema de la alfabetización digital.

se usan sólo para los efectos de validar la identidad y emitir el sentido del voto de cada persona.

Uno de los ejemplos que suele enunciarse a favor de este argumento es que en la actualidad realizamos operaciones bancarias y todo tipo de trámites por Internet "de forma segura". Así, trasladar la realidad electoral a este plano es posible (y razonable) gracias a los avances en materia de seguridad digital, los mismos que hacen viable que utilicemos el *online banking* (o banca por Internet) en la vida diaria. Este argumento se utiliza frecuentemente a nivel internacional y, muy enfáticamente, en el modelo de México analizado en este trabajo.

El argumento es interesante porque traslada de un plumazo el ámbito electoral al contexto digital donde funciona el ámbito bancario, sin preguntarse sobre los costos o implicaciones de ese traslado. Aunque existan similitudes, hay algunas características de cada ámbito que plantean diferencias importantes. Los bancos, por ejemplo, no requieren ser democráticos, pero las elecciones sí. El ecosistema bancario funciona desde la lógica del mercado y como un modelo de negocios, mientras que la democracia y sus principios son independientes al mercado (y muchas veces son límites explícitos a éste).

Los bancos pierden millones de dólares al año como resultado de problemas de seguridad en Internet (fraudes, *hackeos*, etc.), pero eso es sólo parte del negocio, es un costo que deciden pagar porque el beneficio económico al final compensa esas pérdidas inevitables. Tan solo en México, por ejemplo, hubo más de 4.3 millones de quejas de fraudes bancarios por Internet, con pérdidas de 13 mil 977 millones de pesos, de los que se bonificaron el 55% y se resolvieron 88 de cada 100 fraudes a favor de los usuarios, todo esto sólo en el 2018. [15]

El razonamiento utilitarista de costo-beneficio, además, tiene gravísimos problemas para acomodarse en clave democrática, porque ni los derechos ni la democracia están sujetos a ese tipo de valoraciones.[16] Tampoco funcionan como un modelo de negocios y además es inconstitucional e inmoral

15. SUM. "Fraudes financieros provocan pérdidas por 13 mil 977 MDP: Condusef", Informador.mx, 15 de febrero de 2019. Disponible en: https://www.informador.mx/economia/Fraudes-financieros-provocan-perdidas-por-13-mil-977-MDP-Condusef-20190215-0110.html; Forbes. En 2018 hubo más de 4.3 millones de quejas por fraudes cibernéticos en México. 16 de mayo de 2019. Disponible en: https://www.forbes.com.mx/fraudes-ciberneticos-superan-las-4-3-millones-de-quejas-en-mexico/.
16. Dworkin, Ronald. *Taking Rights Seriously*, Cambridge, Massachusetts, Harvard University Press, 1978.

someter derechos fundamentales a la lógica financiera, donde lo que se pierde es meramente un costo a pagar compensado por las ganancias. Pero hay dos diferencias todavía más importantes relacionadas con el tema de la seguridad de los sistemas del VPI y los sistemas bancarios en línea.

Primero, los bancos no se guían ni están obligados por el principio de secrecía en el funcionamiento y diseño de sus sistemas bancarios; muchas de sus actividades funcionan precisamente porque actúan al revés, utilizando mucha información, monitoreando las actividades de sus clientes todo el tiempo. En otras palabras, ven lo que hacemos y realizan registros, comprobantes y rastreos de actividades para mejorar sus mecanismos de seguridad. Al pasar del sistema bancario en Internet al ámbito electoral, la secrecía del voto se vuelve un obstáculo inevitable para el diseño y funcionamiento de cualquier sistema de VPI en este sentido.

Segundo, que cuando un fraude se lleva a cabo en el sistema bancario inevitablemente nos damos cuenta de ello, sea porque podemos detectar gastos que no realizamos o porque el dinero de la cuenta se esfuma. Con el voto por Internet no es posible darnos cuenta de que el sistema fue quebrantado porque la tecnología permite manipular una elección sin dejar rastros; es decir, que si una elección por Internet es fraudulenta, es muy difícil o incluso imposible que nos demos cuenta de ello. [17]

Este último punto requiere que nos detengamos para explicar en detalle los distintos riesgos de seguridad del VPI. Los riesgos pueden dividirse en dos tipos: los que están presentes del lado de los usuarios y los que lo están del lado del sistema.

C-1. Riesgos relacionados con los usuarios del VPI

El primer tipo se relaciona con los usuarios e incluye todos los riesgos que ya existían en los tipos de votación no electrónica, tales como el fraude tradicional (funcionarios e instituciones corruptas que pueden afectar el

17. El punto, en el fondo, es entender que en realidad los sistemas de banca en Internet y los de VPI no son comparables porque las características de seguridad, privacidad y transparencia son estructuralmente diferentes. Al respecto ver: Jefferson, David. If I Can Shop and Bank Online, Why Can't I Vote Online?, Verified Voting, 2019. Disponible en: https://www.verifiedvoting.org/resources/internet-voting/vote-online/. En el mismo sentido: "Los bancos, los minoristas online y otras compañías ofreciendo servicios en Internet toman hasta cierto punto las pérdidas como un costo de hacer negocios online, y generalmente indemnizan a sus clientes frente a los atacantes. El voto por Internet implica un problema mucho más grande: la pérdida de votos es inaceptable", en: Haynes, Peter. "Online Voting: Rewards and Risks", Intel Security, 2014, p. 3.

resultado de una elección) o la compra de votos, más los que son específicos del entorno digital, como son el *hacktivismo*, la posibilidad de los fraudes electrónicos, el robo de identidad e información, el uso de *malware* en los dispositivos utilizados para votar y el interés de los Estados en afectar las elecciones de otros países a través de ciberataques.

Un primer riesgo importante es el de la **coerción**. Durante muchas décadas los sistemas presenciales de votación fueron sofisticándose para evitar que las personas fueran coaccionadas a votar de cierta forma, y para ello una de las medidas fundamentales fue generar un lugar seguro, exento de la mirada externa y que habilitaba un momento privado por completo para que las personas emitieran su voto sin riesgo de que las demás personas pudieran ver el sentido del mismo. La secrecía del voto se fortaleció porque ese espacio permitió realizar ese principio: la persona no podía demostrar por quien votó aunque quisiera hacerlo. El voto por Internet elimina ese lugar seguro otorgado por el Estado y abre la posibilidad de la coerción en el espacio privado.[18]

Vinculado a esta situación está el problema de la **compra de voto**. Si bien sabemos que en las votaciones presenciales esta situación tiene lugar, la compra-venta se vuelve muy fácil de realizar al habilitar un mecanismo remoto alejado de la seguridad de una casilla y de la vigilancia ciudadana. En ambos casos (coerción y compra de voto) la secrecía se pone en juego: cualquier persona que esté presente puede ver por quién se vota al perder el espacio de privacidad otorgado por el Estado. Esto sólo empeora en el ámbito digital.

Ninguna tecnología, ningún dispositivo, es *inhackeable*. Todos los sistemas, aplicaciones y dispositivos son constantemente actualizados y mejorados por el hecho de que pueden ser (y constantemente son) intervenidos o "infectados" con sistemas operativos o *software* maliciosos *(malware)* que permiten operarlos a voluntad de quien logra tomar el control del dispositivo. Más adelante, cuando nos detengamos en el caso de los Estados Unidos de América veremos cómo uno de los últimos estudios especializados en la materia, hecho por la *Academia Nacional de Ciencias,*

18. La coerción puede tomar muchas formas, desde un marido que presiona a su mujer o un padre a sus hijos para votar de cierta forma, o un dueño que obliga a sus trabajadores para votar de cierta manera bajo la amenaza de despedirlos si no lo hacen, hasta la posibilidad de que un grupo criminal obligue a las personas a votar en algún sentido mientras ellos los observan.

Ingeniería y Medicina (ANCIM), concluyó que "no hay en la actualidad ninguna tecnología que pueda garantizar la secrecía, seguridad y verificabilidad de una boleta electrónica transmitida a través de Internet".[19]

El robo de credenciales en Internet es muy sencillo. Al mismo tiempo, es muy frecuente la existencia de sitios en Internet que ponen en peligro los dispositivos de navegación de los usuarios (teléfonos inteligentes, computadoras, tabletas, etc.),[20] así como los casos de ataques directos por *malware* con los que un atacante puede vulnerar directamente un dispositivo para *hackearlo* y tomar control de él. Si un atacante tiene el control de, por ejemplo, tu teléfono inteligente porque utilizó un virus para manipularlo, es muy simple que pueda cambiar tu voto en una elección por Internet, incluso si el sistema cuenta con protecciones de encriptación de extremo a extremo (*End-2-End*), porque la intención del voto de una persona puede cambiarse antes de que el voto salga hacia el servidor de las elecciones (explicamos esto último más adelante). El fraude ni siquiera es detectado y la encriptación se vuelve "irrelevante" en este sentido porque protege una parte del proceso de votación que es posterior a que la manipulación tenga lugar. [21]

C-2. Riesgos relacionados con el sistema de VPI

Los riesgos de las y los usuarios de Internet son sólo una parte del problema. La otra parte se completa con los peligros generales de los sistemas en Internet y los riesgos particulares correspondientes a los servidores con los

19. ANCIM. "Securing the Vote. Protecting American Democracy", September 2018. Disponible en: https://www.nationalacademies.org/news/2018/09/securing-the-vote-new-report. En el mismo sentido ver: Goodman, Rachel y Halderman, Alex J. "Internet Voting is Happening Now. And it could destroy our elections", 15 de enero de 2020. Disponible en Slate: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html. El grupo de trabajo estuvo compuesto por expertos de ciencias de la computación, ciberseguridad, juristas y especialistas electorales, científicos sociales y oficiales electorales.

20. Los casos relacionados con este tipo de vulnerabilidades son más comunes de lo que se cree. En el mercado negro existen personas que se dedican a infectar dispositivos al azar con el único objetivo de vender lo que se conoce como "botnets" o redes de bots, que no es más que el total de los dispositivos infectados a los que el atacante ha ganado cierto grado de acceso. Si otro atacante quiere tomar control de una elección o afectarla de distintas formas, puede comprar estas redes y ganar acceso muy fácilmente a los dispositivos que después puede infectar con *malware* específico para manipular votos o incluso una elección completa. Al igual que otros ataques por Internet, estas acciones son muy difíciles de detectar.

21. Este tipo de riesgos es particularmente grave no sólo porque el uso de *malware* con propósitos ilegales es cada vez más común en asuntos estatales, sino porque este tipo de casos de "ataques escondidos" (donde alguien manipula el voto entre el dispositivo de un usuario y el servidor que recibe ese voto encriptado) ya existe actualmente en los fraudes por Internet que se hacen a bancos *online* en distintas partes del mundo.

que éste funciona. Los sistemas pueden ser afectados por "ataques internos" o por "ataques externos". Los del primer tipo corresponden a casos en donde la misma autoridad electoral u otro sujeto involucrado en el armado del *software o hardware* o de echar a andar el sistema, infecta el sistema para realizar un fraude.[22] Hacer esto es tan simple que una sola persona atacando alguno de los muchos elementos vulnerables puede provocar una falla de seguridad tal que todo el sistema (y con él las elecciones) se comprometa.[23]

El segundo subtipo de riesgos (externos) puede vulnerar un sistema de VPI de distintas formas. Al funcionar en Internet, los sistemas de votación pueden ser atacados para provocar la denegación del servicio -los conocidos ataques DDoS- e impedir, por ejemplo, que las personas puedan usarlo (impidiendo votar). Otra forma de intrusión remota es la que se hace cuando un atacante externo logra robar información que le permite tomar control del sistema, tal como sucede en los casos de los ataques APT o de Advertencia Persistente Avanzada (*Advanced Persistent Threat*).

Tanto las empresas más poderosas y mejor preparadas en términos de seguridad como Google, como las instituciones mejor equipadas para lo mismo como el Pentágono, han sido víctimas de este tipo de ataques, perdiendo información delicada. El peligro de estos ataques es que mientras más poderoso sea el sujeto que los realiza (en términos económico-tecnológicos), más fácil es realizar el ataque con éxito (y más difícil detectarlo).[24]

22. En muchas ocasiones los sistemas de VPI se echan a andar con dispositivos que están sujetos a este tipo de riesgos. En el caso de la Ciudad México (2020) analizado más adelante, veremos como uno de los riesgos detectados en un informe posterior a la elección señala la utilización de una computadora personal de uso diario de funcionarios del IECM; es decir, que no fue designada ni auditada ni protegida especialmente para la jornada electoral. En teoría, si la computadora estuviera infectada con un *malware* para tomar el control del sistema de VPI y después manipular la elección, ese uso descuidado habría sido suficiente para lograrlo.

23. Goodman, Rachel y Halderman, Alex J. "Internet Voting... "*op. cit*. Para operar un sistema de VPI en una jornada electoral se necesitan tanto de funcionarios que realicen los procedimientos para echarlo a andar como de dispositivos para realizar ciertos procesos indispensables para la elección. En el caso del VPI de la Ciudad de México, intervienen distintos funcionarios en varias etapas del proceso y se utiliza una memoria USB y una computadora portátil para realizar procesos necesarios de la jornada electoral. Esto abre riesgos típicos a cualquier modalidad de elección (tanto presencial como remota) pero con la diferencia de que en Internet es mucho más fácil manipular una elección en su totalidad, con la consecuencia de que los votos sean borrados, de que su sentido sea cambiado a gran escala y de que las preferencias de las personas sean expuestas.

24. En estos casos y el de los DDoS, si los ataques son exitosos -a diferencia de lo que sucedería con el robo del voto postal o de alguna urna-, es posible afectar toda una elección con un esfuerzo mucho menor (esto es lo que se conoce como "a small conspiracy for cyber tampering and a wholesome fraud"). Norden, Lawrence. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost,* The Brennan Center for Justice, New York University, 2006; Halderman, Alex. *Hacking the D.C. Internet Voting Pilot*, Freedom to Tinker, June 2012. Disponible en: https://freedom-to-tinker.com/2010/10/05/hacking-dc-internet-voting-pilot/.

Para explicar claramente los riesgos externos debemos dividirlos de acuerdo a: a) lo que sucede en los componentes del sistema, en particular los servidores de las elecciones; para luego b) explicar las limitaciones de los sistemas que prescinden del uso de papel y las razones por las que se desaconsejan a nivel internacional.

a. La seguridad de los servidores del VPI

Todos los sistemas de VPI necesitan servidores de Internet que les permitan desarrollar su sistema de votación y recibir la información del mismo. Los servidores sirven, por así decirlo, como respaldo de la aplicación de Internet con la que las personas votan. También son indispensables para etapas del proceso como el pre-registro de la elección, ya que todos los datos de las personas que van a votar por este medio quedan almacenados en ellos. Pero esto no es todo, porque los servidores también intervienen una vez que el voto fue emitido al recibir los votos encriptados y para almacenarlos hasta el momento en que la jornada electoral termina y se cierra la elección para proceder al conteo.[25]

Ningún servidor es invulnerable ni 100% seguro porque ninguna tecnología es infalible ni perfecta. Como no existe un sistema de seguridad completo o total que los vuelva invulnerables, un sujeto con suficiente poder de ataque puede ganar el control administrativo de los servidores de respaldo. ¿Qué pasaría si esto sucede? Que podrían acceder a la información suficiente para reconstruir una elección, quitarle el anonimato a los votos y alterarlos para cambiar un resultado (sin que nadie pueda darse cuenta).[26]

25. Los servidores son, en este sentido, equipos y programas (*hardware y software*) de computadora que realizan tareas de almacenamiento de datos, información y recursos de *hardware* y *software* de los usuarios en Internet (entre otros). Hay de distintos tipos y desempeñan distintas funciones (almacenar datos, correos, juegos, aplicaciones, etc.). En el caso del VPI, se utilizan servidores de votación que, en teoría, verifican que el contenido de los votos que son encriptados una vez que se emiten, sean válidos sin necesidad de descifrarlos (funcionan como una especie de urna virtual).

26. Este fue uno de los puntos subrayados por el MIT (Massachusetts Institute of Technology), uno de los centros de investigación más importantes del mundo especializado en la materia, cuando emitió su reporte sobre la seguridad del voto electrónico en EUA, tal como explicaremos en el apartado correspondiente. Al respecto ver: Specter, Michael; Koppel, James & Weitzner, Daniel. *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, The First Internet Voting Application Used in U.S. Federal Elections*, report from MIT researchers. Disponible en: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213. Para la nota del MIT al respecto ver: *MIT News Office. MIT researchers identify security vulnerabilities in voting app,* February 13, 2020. Disponible en: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.

Realizar ataques DDoS es relativamente simple[27] porque es fácil rentar ejércitos de bots para saturar un sistema de votación el día de la elección (utilizar las redes de bots o comprar *botnets* tal como mencionamos más arriba), por eso las agencias utilizan servicios de mitigación como *Cloudflare* o *Imperva*. El problema es que para que un servicio de mitigación sea efectivo, debe espiar el tráfico para detener el ataque; es decir, que debe desencriptar el tráfico entre los usuarios y los servidores para saber cuál tráfico corresponde a la elección y cuál no.

La forma de hacerlo es a través de un *Transport Layer Security* (TLS) [28]en el que se realiza un "ataque de intermediario" con permiso. Los TLS son tecnología de encriptación que habilita la protección "HTTPS" que garantiza la confidencialidad del tráfico de información en el sistema. La seguridad suele vulnerarse por lo que se conoce como un "ataque de intermediario" o "*man-in-the-middle attack*", que funciona para robar las credenciales del votante y modificar sus elecciones electorales. Lo anterior puede pasar de distintas formas: una de ellas es cuando se logra tomar control o robar las llaves de encriptación del TLS que están en los distintos servidores; tomar el control de alguno de ellos permite obtener la llave y acercarse a cambiar una elección.[29]

El peligro no es teórico, se ha demostrado que un sujeto con suficiente poder, tal como sería un Estado o alguien con un poder económico similar, podría obtener las credenciales para realizar un ataque de intermediario al comprometer uno de los servidores.[30]

27. Un ataque DDoS implica usar un gran número de conexiones para inundar o saturar el sitio web que se busca atacar, sobrecargando el sistema e impidiendo que los usuarios legítimos puedan usarlo. Culnane, Chris; Eldridge, Mark; Essex, Aleksander; Teague, Vanessa. *Trust Implications of DDoS Protection in Online Elections*, CSCR, 3 August 201, p. 2. Disponible en: https://arxiv.org/pdf/1708.00991.pdf. Uno de los casos conocidos al respecto es el del ataque masivo realizado supuestamente por Rusia a Estonia en el año 2007, que fue tomado la OTAN (Organización del Tratado del Atlántico Norte) como una cuestión de seguridad y donde se desplegaron especialistas para contrarrestar acciones de "cyber-terrorismo". Al respecto ver la investigación realizada por el diario The Guardian en esas fechas: https://www.theguardian.com/world/2007/may/17/topstories3.russia.
28. Los TLS son un grupo de protocolos criptográficos para la seguridad de las comunicaciones en Internet que proveen confidencialidad, integridad y autenticación a una red de comunicaciones en Internet en la capa de aplicación. Existen distintos tipos de ataques directos a TLS en cuanto a sus componentes y, además, el tipo de ataque particular "*TLS Stripping*" que se utiliza para evitar la conexión TLS en primer lugar. Cardillo, Anthony & Essex Aleksander. "The Threat of SSL/TLS Stripping to Online Voting", Springer, 2018, p. 37.
29. J. M. Porup. Online voting is impossible to secure. So why are some governments using it?, CSO, May 2 2018. Disponible en: https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html.
30. Culnane, Chris... *op. cit.*

¿Cómo se realiza este tipo de ataque? Los atacantes logran que un usuario entre al sistema con un URL (cotidianamente conocido como el "*link*" o dirección única de la página en Internet) que no tiene la seguridad "HTTPS" sino que, por ejemplo, es una dirección "HTTP", lo que significa que el usuario entra a un canal que no está encriptado, donde el atacante puede suprimir la respuesta de un servidor TLS cuando intenta redirigir al usuario al canal seguro ("HTTPS"). Si el atacante lo logra, puede ver y hacer cosas sin que el sistema detecte esa intervención. Un serio problema de dicha posibilidad es que este tipo de ataques en contextos de VPI está sub-analizado, aunque hay suficiente evidencia que apunta a la existencia de vulnerabilidades serias en TLS en los sitios web de distintos países utilizados para los pre-registros electorales y para la votación en general también.

Así, un atacante puede intervenir en la página de Internet de las elecciones con una "*TLS Stripping*"; una acción para ponerse en el medio del usuario y la página para robar las credenciales de una votante (por ejemplo, cuando la página pide que ponga el usuario y su contraseña). Después, si la votante marca un voto por una candidata (presiona "Votar"), el intermediario que tomó control podría cambiar su voto simplemente intercambiando los nombres de la boleta o cambiando directamente la elección de la persona.[31] Por esta razón se han generado protecciones criptográficas para mitigar estas vulnerabilidades, aunque hay estudios que demuestran claramente cómo es posible inyectar *software* que permite el robo de votos (incluso utilizando mecanismos de "fuerza bruta" para romper la seguridad).[32]

Otra forma de mitigación de riesgo es con factores de autenticación múltiples como sucede en el caso de Estonia (que explicamos más adelante), como puede ser un *software* específico en una aplicación y una credencial digital para firmar los votos. Sin embargo, incluso estos mecanismos

31. Cardillo, Anthony... *op. cit.*, pp. 35-36. Un ejemplo simple para entender a qué nos referimos sería el siguiente: imaginemos que el sitio protegido con encriptación para una elección por Internet es "https://eleccionsegura.com". Este tipo de acciones se realiza cuando un atacante hace que un usuario entre a un sitio espejo que no es HTTPS, como sería: "http://eleccionsegura.com". Hay mucha evidencia de que la ciudadanía promedio no se percata de esta diferencia ni conoce las implicaciones de seguridad, haciendo muy sencillo realizar este tipo de ataques.

32. Para la posibilidad del uso de ataques de fuerza bruta ver: Culnane, Chris... *op. cit.*, pp. 127–145. Para la demostración sobre las fallas de seguridad y el rompimiento de la seguridad criptográfica ver: Halderman, J.A.; Teague, V.: The New South Wales iVote system: security failures and verification flaws in a live online election. In: Haenni, R., Koenig, R.E., Wikstrom, D. (eds.) VOTELID 2015. LNCS, vol. 9269, Springer, Cham (2015), pp. 35–53.

pueden ser vulnerados porque tanto la aplicación para votar como el ID del *software* son descargados desde Internet en un buscador que está sobre un TLS. El riesgo de que esto suceda tampoco es hipotético, tal como muestra este caso, que utiliza esas formas de mitigación sin poder evitar los riesgos de seguridad.

Corregir estas vulnerabilidades no es sencillo porque la tarea de corrección sólo puede hacerse cuando se han identificado primero; cuando la autoridad o la empresa encargada del sistema de VPI está al tanto y toma acciones para resolverlas. Para las y los usuarios es difícil detectarlas porque los buscadores no generan avisos de posibles riesgos de seguridad (advertir, por ejemplo, que se utiliza una dirección "http://" y no una "https://, o que la página no tiene el símbolo del candado en la barra de direcciones) y muchos estudios señalan que no están al tanto de esos detalles o que no los consideran riesgosos.[33]

El problema es acumulativo, los riesgos en una dimensión se suman a los de otra y así sucesivamente hasta dejar una situación compleja de inseguridad. No sólo se trata de los peligros de la seguridad tecnológica que pueden ser aprovechados por un *hacker* o un grupo criminal con suficiente poder para contratar a un equipo que lo haga, sino también de la posibilidad de que otro gobierno o un sujeto privado extranjero con poder económico similar se haga de los medios para tomar control de un sistema y usarlo a su favor. Todo esto sin mencionar los riesgos internos de los que ya hablamos, en los que una mínima corrupción de la agencia que controla el sistema de VPI o de una empresa que sea relevante en la producción de *software* o *hardware* para el mismo (servidores, llaves, dispositivos, etc.) puede ser suficiente para poner en riesgo una elección entera.[34]

Finalmente, es importante mencionar que los estándares sobre la seguridad electrónica en el voto por Internet no suman para reducir el problema. No hay un set que centralice o uniforme cuáles son las reglas concretas por las que un sistema de VPI es satisfactorio en todos los puntos

33. Cardillo, Anthony *op. cit.* Los distintos estudios (analizando más de 100 sitios de elecciones en Internet) muestran que en muchos casos la difusión de las propias páginas de Internet por parte de las autoridades o los candidatos ponen en riesgo la seguridad de una votación y que muchos de los sitios encontraron numerosas vulnerabilidades de seguridad TLS
34. J. M. Porup... *op. cit.*

que mencionamos, sino que hay una realidad de criterios descentralizados que dependen más o menos del país de que se trate o del área tecnológica de la que se trate, y que siempre están sujetas al avance vertiginoso de la tecnología que cuestiona y pone en jaque los criterios de seguridad todo el tiempo.

b. El lugar del papel como elemento de seguridad para las elecciones

Como los sistemas de voto por Internet no utilizan ningún respaldo en papel (no hay ningún comprobante que diga de qué manera voté), cuando una persona vota debe confiar ciegamente en que el sistema funciona como le dijeron que funciona y en que su elección electoral terminará reflejada en el resultado final. El problema es que, si la elección es *hackeada* y los votos se manipularon, no podemos saber si los votos se cambiaron porque el *hackeo* no deja rastros para darnos cuenta de ello. Comprometer el resultado final de una elección por completo es, tal como advirtieron en otro estudio este mismo año las principales agencias de seguridad de EUA[35], una posibilidad real porque las computadoras sólo permiten ver los errores que son imposibles de justificar o que son muy obvios en cuanto al objetivo de manipular la elección.[36]

La conclusión es similar a varias de las recomendaciones del reporte de la ANCIM, mencionado más arriba:

35. El reporte fue preparado por: FBI (*Federal Bureau of Investigations*), la Agencia 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. Informe: "Risk Management for Electronic Ballot Delivery, Marking, and Return". Disponible en: https://s.wsj.net/public/resources/documents/Final_%20Risk_Management_for_Electronic-Ballot_05082020.pdf. Una de las conclusiones finales del mismo fue que: "En el tiempo presente, el Internet (o cualquier red conectada al Internet) no debe ser utilizada para el regreso de las boletas electrónicas marcadas [con los votos emitidos]". Ver: NPR. *Feds Warn States that Online Voting Experiments are "High Risk"*, by Miles Parks. May 11, 2020. Disponible en: https://www.kuow.org/stories/feds-warn-states-that-online-voting-experiments-are-high-risk.

36. En los sistemas de VPI, los mecanismos para lograr la secrecía del voto posibilitan que los votos sean manipulados en secreto sin ser detectados (lo que se conoce como *secret ballot-secret tampering*). A diferencia de otros sistemas en Internet como las redes sociales o las bancas en línea (*online banking*), un ataque que roba las credenciales de un votante o que modifica su voto es más difícil de detectar y corregir precisamente por la forma en que los sistemas de VPI funcionan para proteger la secrecía del voto. Explicamos esto en detalle el siguiente punto. Cardillo, Anthony & Essex Aleksander. "The Threat of SSL/TLS Stripping to Online Voting", *Springer*, 2018, p. 36.

> Las elecciones deben realizarse con boletas de papel legibles por humanos. Al tratarse de evidencia que no puede manipularse vía *software* ni *hardware* pueden utilizarse para auditar y verificar los resultados de una elección. Además señaló que "Las máquinas de votación que no habiliten la capacidad de ser auditadas independientemente -por ejemplo, las máquinas que no producen una impresión de la elección del votante que puedan ser verificadas por éste y usadas en verificaciones- deben ser removidas del servicio lo más pronto posible".
>
> El voto por Internet no debe ser usado en la actualidad y tampoco debe ser usado en el futuro hasta que y sólo cuando se desarrollen y existan garantías de secrecía, seguridad y verificabilidad. Al momento, ninguna tecnología puede garantizar la secrecía, seguridad y la verificabilidad de una boleta electrónica transmitida por Internet.[37]

Las elecciones sin respaldo en papel no pueden auditarse manualmente. Los mecanismos de recuento de los sistemas de VPI son parte del mismo sistema que es vulnerable a los riesgos tecnológicos y, sin el respaldo en papel, no pueden garantizar que el sentido final de los votos electrónicos es el que fue otorgado por los votantes (una vez que un sistema es manipulado, el recuento electrónico también puede manipularse). [38]

Si está en riesgo la posibilidad de verificar que los votos son contados de acuerdo a como se emitieron (*counted as cast*), el principio de integridad del voto también. A fin de cuentas, demostrar la correspondencia entre la intención de un voto y su conteo, tenemos que confiar ciegamente en que el *software* hace lo que nos dicen que hace porque no podemos verlo por nosotros mismos. [39]

D. ¿La secrecía del voto puede garantizarse en Internet?

Quien defiende el voto por Internet señala siempre que una de las oportunidades que da el avance de la tecnología es que hoy en día tenemos

37. ANCIM. "Securing the Vote..." *op. cit.*
38. Sucede lo mismo con el conteo inicial de una elección. Cuando la jornada electoral por Internet inicia, siempre hay una revisión para verificar que las urnas virtuales están vacías con cero votos (porque la elección aún no comienza) como medida de seguridad. Sin embargo, esto no garantiza la seguridad del sistema si el mismo ya fue *hackeado*. Es perfectamente posible manipular un *software* para que diga lo que sea que le pidan que diga; es decir, que sea programado para mostrar que no está manipulado aunque sí lo esté. Simplemente habría que programarlo para mostrar que el sistema tiene cero votos cuando en realidad ya fue programado para cambiar el resultado final (la garantía del conteo en cero es estética, no significa que el sistema sea íntegro).
39. El análisis de los sistemas de VPI ha dado paso al concepto de "independencia del *software*" (*software independence*), que consiste en que todo el *software* que se utilice en una elección debe cumplir la condición de que, cuando haya algún cambio o error no detectados en él, estos no se traduzcan en un cambio o error indetectable en el resultado de la elección. El problema es que la tecnología con la que contamos hoy hace que los sistemas de VPI no puedan cumplir esta condición.

herramientas que nos permiten garantizar la secrecía del voto porque separan el sentido del voto de la identidad del votante. La separación se realiza por medio de un *software* que realiza la mezcla o alternación (*mixture*) aleatoria de los votos, por lo supuestamente no es posible saber cómo votan las personas.

La secrecía del voto implica que nadie puede saber cómo votamos, pero no sólo esto: significa que no pueden saberlo incluso si intentamos demostrar cómo votamos. Con la boleta en papel, por ejemplo, podemos decirle a una persona que votamos por alguna opción política pero al no poder ver el contenido de la boleta ni estar presente dentro de la casilla electoral, no puede cerciorarse de que esto es así.[40] El problema del voto por Internet es que por la forma en que la tecnología funciona, el principio de secrecía tira en una dirección opuesta a la integridad del voto (en relación a la seguridad). A esto se le conoce como el **dilema secrecía-integridad**. ¿En qué consiste este dilema?

En que las acciones que protegen la integridad del voto, tal como podría ser dar un recibo del sentido del voto o hacer la contabilidad de dónde entra y dónde sale la información en el sistema, ponen en juego la secrecía del voto: si me dan un recibo que dice por quién voté para utilizarlo en caso de un recuento, cualquier persona que lo obtenga puede ver cómo voté. Mientras que las que protegen la secrecía (tal como no dar ningún recibo para evitar el problema anterior) hacen que la integridad se ponga en juego.

Más arriba explicamos que cuando se usan servicios de mitigación para proteger una elección de ataques DDoS, es posible tomar control de ese servidor y que, si un sujeto con suficiente poder realiza un ataque y gana control del servidor, puede espiar la forma en que las personas votan (porque puede ver el tráfico de información) o simplemente tomar control y cambiar el sentido de los votos.[41] La posibilidad de que eso suceda también ha sido demostrada de forma contundente (no es una hipótesis). Expertas y especialistas en ciencias de la computación demostraron que la defensa en contra de ataques DDoS requiere de la vigilancia de la información de

40. Incluso objetando que hoy es posible grabar un video marcando la boleta electoral para mostrarlo luego (en un contexto de ejemplos de compra de voto, por ejemplo), la persona podría cambiar la opción o anular el voto después de grabar el video, para votar de acuerdo a su conciencia y después depositarlo en la urna. El punto de la secrecía es, en última instancia, contar con la posibilidad material de que la intención del voto no sea descifrada en definitiva.
41. J. M. Porup. Online voting... *op. cit.*

la elección y pone en riesgo el secreto del voto (este análisis se hizo en el contexto de las elecciones de Australia en el 2017).[42]

La exposición de la información no sólo es peligrosa en casos de atacantes. Cuando el tráfico de votos puede intervenirse, el sujeto que está en control de la información puede conocer las preferencias electorales y utilizarlas de formas que vulneran los derechos, tal como sucede al hacer amenazas políticas (en Venezuela ya sucedió que el Presidente Nicolás Maduro amenazó a la población diciendo que sabían cómo habían votado y que tomarían medidas al respecto), o con el simple hecho de vigilar a las personas porque se conocen sus preferencias políticas (ver quién vota, cuándo vota, si vota o no e, incluso, ver a quién vota). El riesgo de la vigilancia no es menor en un contexto de creciente vigilancia estatal como el de México y muchos otros países en el mundo.[43] En el mismo sentido que con la vigilancia estatal, los riesgos para la secrecía también son especialmente graves en países con problemas serios de violencia de género, donde perder un espacio protegido para votar y en cambio votar en la esfera privada puede poner en una situación de mayor vulnerabilidad a las mujeres o abrir mayores oportunidades para la coerción en el seno familiar.[44]

E. ¿Se trata de un sistema más transparente?

Otra promesa apoyada en la tecnología del VPI es que todo el sistema puede ser auditado, que todos los procedimientos pueden ser visibles y que también pueden ser evaluados de forma completa.

42. Culnane, Chris... *op. cit.* En el mismo sentido: "La elección estatal de NSW [New South Wales] del 2015 fue tan insegura que uno de los escaños en la Cámara Alta del Parlamento pudo haber sido decidida por votos *hackeados*. En respuesta al escándalo, la Comisión Electoral optó a grandes rasgos por evitar la transparencia sobre los temas de seguridad que Teague y su equipo reportaron, y sólo revelaron la naturaleza real del problema en cuestionamientos cerrados frente al Parlamento un año después", en: J. M. *Porup. Online voting... op. cit.* En específico y sobre los resultados electorales, Vanessa Teague señaló que: "No hubo advertencias en el buscador. El ejercicio trastocó exitosamente la conexión TLS del servicio de de la tercera parte involucrada. **Se hubiera visto completamente normal del lado de la Comisión Electoral. Se hubiera visto exactamente que un voto legítimo.** Fue un voto legítimo de un votante elegible. Sólo que no fue el voto que el votante intentó emitir".

43. R3D: Red en Defensa de los Derechos Digitales, *El Estado de la Vigilancia: Fuera de Control*, México, Noviembre de 2016. Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf.

44. La variable del género debe ser siempre tomada en cuenta por las obligaciones estatales de protección y garantía de los derechos de las mujeres. En este caso, el voto remoto puede ponerlas en la situación de ser presionadas para votar en cierto sentido (por ejemplo, que el marido, padre o pareja presione para votar por un candidato determinado) o en la situación de ser maltratadas por su elección electoral (sin mencionar la facilidad con la que, en la ausencia de un espacio seguro como el de una casilla electoral y en un caso como el que planteamos, la persona que coacciona o maltrata podría utilizar el dispositivo de la votante (su celular, por ejemplo) y votar en lugar de ella.

Sabemos que hay muchas partes de los sistemas de VPI que funcionan de manera automática, lo que significa que la forma en la que la transparencia se materializa en estos casos es distinta a la que normalmente se da en los procesos electorales presenciales (que las y los observadores electorales y los representantes de los partidos políticos puedan ver y estar presentes en todos los momentos del proceso). La transparencia queda atrapada dentro de una "caja negra" porque no sabemos cómo funciona el *software* ni podemos ver los procesos que realiza.[45] En el caso de un recuento de una votación por Internet, por ejemplo, no podemos contar ni observar materialmente, sino que simplemente veríamos los resultados que arroja una computadora después de realizar su recuento, de acuerdo al *software* del sistema de VPI.

¿Cómo podemos asegurarnos de que algo cumple lo que promete cuando no podemos ver aquello que supuestamente es transparente? La mayoría de los sistemas de voto por Internet no son de fuente abierta (open source), lo que significa que la investigación del código fuente y de todos sus componentes no es posible.[46] Las personas deben de conformarse con auditorías que normalmente son financiadas con millones de pesos (o dólares) que se hacen con empresas o entes públicos y que se utilizan para legitimar un sistema que no permiten revisar de forma independiente en este sentido fuerte. Normalmente no hay lugar para realizar lo que se conoce como "pruebas de penetración y recompensa" ni para que los especialistas independientes revisen la fragilidad o las fortalezas del sistema más allá de las auditorías controladas por las autoridades.[47]

El hecho de que el *software* de un sistema de votación sea de fuente cerrada es un problema grave porque imposibilita llevar a cabo acciones que nos permitirían saber si los sistemas son tan seguros como prometen serlo. La ingeniería inversa (*reverse engineering*), por ejemplo, no está

45. J. M. Porup. Online voting... *op. cit*
46. Para dimensionar la importancia de la revisión independiente del código fuente podemos ir a la experiencia realizada con el sistema de VPI en Washington, D.C., en el año 2012. En este caso las autoridades abrieron por primera vez el sistema que iban a usar para que fuera revisado por expertos independientes quienes, al revisar el código fuente, se dieron cuenta de un error menor que les permitió ganar el control del sistema por completo y modificar los resultados de la prueba piloto. Los realizadores del *software* utilizaron en una de las líneas de código comillas dobles ("") en vez de comillas simples (") al momento de escribir un comando. Este error mínimo fue suficiente para perder el control y para que las elecciones fueran *hackeadas*. Al final, las autoridades cancelaron el uso del voto por Internet para esas elecciones. Halderman, Alex. *Hacking the D.C... op. cit.*
47. J. M. Porup. *Online voting... op. cit*

avalada al momento de las auditorías (tampoco el *hackeo* ético para buscar vulnerabilidades), a veces por alusión a motivos de propiedad intelectual, otras veces porque este tipo de acciones están penalizadas por ley y, en otros casos, simplemente porque las auditorías se enfocan en la funcionalidad del sistema más que en probar seriamente en condiciones de alto riesgo la seguridad.

Además, las auditorías normalmente están condicionadas por acuerdos de confidencialidad *(non-disclosure agreements*) que prohíben hacer públicos ciertos hallazgos que sólo son comunicados de manera privada a la empresa o a la agencia que se encarga del sistema. El resultado es que nadie puede saber a ciencia cierta cómo funciona el sistema ni si funciona como dicen que funciona, porque no es transparente: "Esto es exactamente lo opuesto a cómo funcionan las elecciones basadas en papel: todas las personas saben y entienden cómo funciona el sistema, e incluso pueden ir y observar los conteos de las boletas si así lo desean".[48]

La falta de transparencia impide que una parte del sistema electoral esté sujeta al escrutinio público y esto afecta otros principios fundamentales de las elecciones como el de publicidad. No se trata solamente de que las personas especializadas en la materia puedan revisar que lo que dicen las autoridades es cierto, sino de que las personas puedan entender y escrutar la forma en que el sistema funciona.[49] Más adelante, cuando analicemos el caso del voto electrónico en Alemania, veremos que existen cuestiones normativas que se vuelven fundamentales en este punto. Cuando no podemos ver lo que pasa dentro de esa "caja negra" del voto por Internet, el riesgo es transversal: incluso la integridad del voto se pone en juego porque, en caso de una elección fraudulenta, no podríamos darnos cuenta de ello porque no podemos ver nada.[50]

El tema de la transparencia es paradójico porque las autoridades consideran que las auditorías son suficientes para garantizar este principio, aunque en realidad la mayoría de las veces no cuentan con el tiempo

48. *Idem.*
49. Los sistemas de VPI son mucho más difíciles de estudiar en general. No sólo en cuanto a su estructura sino también a su funcionamiento el día de la elección. Halderman, Alex J. Security Analysis of Estonia's Internet Voting System, 31st Chaos Communication Congress (31C3), Hamburgo, Alemania. Diciembre de 2014. Disponible en: https://www.youtube.com/watch?v=kdR3-10d2EQ&feature=emb_title.
50. Sebes, E. John. A hackes case for election technology, OSET Institute, August 6 2013. Disponible en: https://www.osetfoundation.org/blog/2015/8/6/a-hacked-case-for-election-technology.

suficiente para analizar la totalidad del sistema o no pueden acceder a todos los componentes del mismo (a veces sólo pueden ver parcialmente el código, otras veces sólo analizan el funcionamiento pero no son libres para buscar otro tipo de vulnerabilidades, etc.). La limitación es relevante porque el hecho de que en una auditoría superficial no se encuentren vulnerabilidades **no significa que no las haya**. Es perfectamente posible que un atacante con más tiempo, más recursos o incluso más suerte que quienes hacen la auditoría pueda dar con ellas y rompa los elementos de seguridad.

Si la confidencialidad hace que los errores y los riesgos de seguridad no sean públicos o si los formatos de las auditorías hacen que estos no se reporten, entonces es imposible darnos cuenta de si existieron intentos de *hackeo* anteriores (y si estos tuvieron éxito). En el apartado en que analizamos el sistema de VPI del IECM veremos cómo todas las auditorías que se han llevado a cabo tienen alguno o varios de estos problemas, y cómo los principios de transparencia y publicidad están seriamente afectados.

La transparencia y la publicidad de las elecciones están pensadas también para que las personas confíen en los procesos electorales, las instituciones y la democracia. Hay algo particularmente malo cuando la opción que da un sistema es la de obligar a confiar ciegamente en la tecnología o en lo que las autoridades nos dicen que hace esa tecnología.

F. ¿Es más económico que otras alternativas?

Organizar elecciones es costoso y quienes impulsan el VPI señalan que la tecnología puede evitar el gasto excesivo al sustituir otras modalidades de votación (ahorrar en recursos humanos, en gasto de producción de boletas e infraestructura de votación presencial, etc.). Dichos costos deben ser evaluados de manera integral por varias razones: primero, porque no debe contarse sólo el costo del *hardware* y del *software* sino del reemplazo permanente de estos; segundo, porque debe pensarse también en el costo de manutención de los equipos así como en el de actualización del *software*; y tercero, porque el costo anual de operación del sistema debería contemplar también la operación del sistema, la capacitación de las y los funcionarios y los gastos en auditorías, educación digital y comunicación ciudadana sobre el uso del mismo.

Normalmente las estadísticas sobre costos no incluyen estos datos y presentan sólo el costo de la preparación del sistema y de sus componentes de *hardware* y de *software.* Todo esto es importante sobre todo cuando entendemos que el costo inicial de un sistema de votación representa un porcentaje pequeño del gasto que se tiene que hacer a mediano y largo plazo tomando todas las modificaciones, correcciones y actualizaciones que requiere la tecnología. [51]

Los matices y formas de evaluar los costos de un sistema son el reflejo de un problema estructural: que no existe una metodología definitiva ni estandarizada sobre la forma de medirlos que haya generado un consenso hasta ahora. Un detalle particular es que estos sistemas contienen "costos escondidos"[52] (*hidden costs*) que son difíciles de evaluar e incorporar a la medición total o que no contabilizan la infraestructura pública preexistente en la que el sistema se apoya porque puede utilizarse para él, aunque esto pueda poner en riesgo la seguridad del sistema.[53]

Una variable que suele utilizarse y es importante para evaluar los costos de un sistema es el número de votantes que lo utiliza: si un sistema es utilizado por muy pocos votantes, el costo-beneficio del mismo se afecta, a diferencia de si el sistema es utilizado por muchos votantes. Lo que esta proporción muestra, es que la evaluación de los costos año por año puede ser también variable cuando se toma este criterio (que es internacionalmente utilizado para medir el costo-beneficio de los sistemas para votar, incluido el de Internet) relacionado con la participación política (y que, si el sistema es poco usado, puede resultar costoso aún así tomando todo esto en cuenta).[54]

51. Norden, Lawrence. *The Machinery of Democracy…" op. cit.,* p. 9
52. Un buen ejemplo se relaciona con el problema de la seguridad. Ante la necesidad, normalmente no contemplada, de comprar equipos electrónicos totalmente nuevos y de uso exclusivo para el sistema (para evitar los riesgos de uso de *malware* en ellos y de la manipulación de la elección), los costos de un sistema pueden elevarse significativamente, aunque esto no suela tomarse en cuenta. La realidad de muchos sistemas de VPI, tal como sucede con el del IECM, es que dependen en gran parte de la infraestructura pública para funcionar (y para reducir costos), pero esta infraestructura no se utiliza únicamente para el sistema de VPI sino que es de uso corriente (una computadora personal del Secretario General a cargo de cargar las llaves criptográficas, por ejemplo). El costo escondido muestra dos cosas: primero, que no es contabilizado y, segundo, que esa falla de planeación tiene costos a nivel de la seguridad del sistema como un todo.
53. Krimmer, Robert; Duenas-Cid David; & Krivonosova, Iuliia. "New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?", *Public Money & Management*, 2020, pp. 2-3.
54. *Ibidem*, pp. 6-7. Esto es así porque la evaluación costo-beneficio toma los recursos consumidos en el uso de un sistema frente a la cantidad de gente que lo usa, lo que vuelve a la participación política un elemento a tomar en cuenta.

Finalmente, el VPI debe ser una medida complementaria a los otros medios de votación (presencial o postal) si no se quiere correr el riesgo de privar del voto a personas en situación de vulnerabilidad, de analfabetismo digital o a las que elijan votar por otros medios ante, por ejemplo, la desconfianza en la seguridad del sistema de VPI. En este sentido, el costo por un nuevo canal de participación deberá evaluarse en muchos casos -salvo que se contemple como un sustituto de las otras formas de votación- como un gasto extra a los gastos preexistentes. Esto último abre un debate sobre si en verdad es necesario realizar esos gastos o si sería mejor invertirlos para que los sistemas más seguros (en caso de demostrar que el VPI no lo fuera, tal como sostenemos en este trabajo) que están fuera de Internet funcionen de manera más eficiente.[55]

Si vamos nuevamente a la experiencia del SEI del IECM y a la información disponible al respecto, podemos hacer un balance de los costos frente a los supuestos beneficios frente a la participación obtenida en los distintos ejercicios. Para hacer el balance tomamos el costo aproximado del SEI en el año 2017 por ser el único disponible de la información pública otorgada por el IECM y disponible en su página.

El costo del SEI para el 2017 se desglosa por el IECM de la siguiente manera: 1) costos fijos de un total de $8,450,000.00 pesos; 2) costos operativos de un total de $1,496,957.89 pesos; 3) costos variables que iban desde $3,593,700 pesos (si lo usaban 6000 electores) hasta $25,754,850 pesos (si lo usaban 43000 electores). Esto implica un total que va desde $13,814,393.89 pesos (pensando en el uso del SEI por 6000 electores) hasta 35,975,489.89 pesos (pensando en el uso del SEI por 43000 electores), con un tipo de cambio de 18.69 pesos por dólar al 31 de mayo de 2017. Obviamente estos costos deberían modificarse si quisiéramos actualizar el balance y, además, a las modificaciones que el SEI ha sufrido probablemente impacten de un modo u otro en el costo total (la información proporcionada por el IECM no incluyó estos datos). ¿Qué balance tenemos?[56]

Como mencionamos en el apartado sobre la participación política más arriba, la experiencia de la Ciudad de México no muestra un aumento

55. Wells, Peter. *The cost of online voting,* Hackernoon (blog), November 11th 2017. Disponible en: https://hackernoon.com/the-cost-of-online-voting-dbca9e382c78.
56. IECM, *Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación,* Ciudad de México, 2017, pp. 24-28 (páginas 47-51 del documento en .pdf). Disponible en: https://www.iecm.mx/www/taip/cg/acu/2017/IECM-ACU-CG-014-2017.pdf.

concluyente en la participación sino más bien la tendencia sostenida de que las personas utilizan en mayor medida el voto postal para votar de forma remota (con el mejor ejemplo de la elección de la Jefatura de Gobierno del 2018, que sin tener habilitado el VPI tuvo la mayor participación política de la historia reciente desde el extranjero). Además, incluso habilitada, muy poca gente la usa de manera remota y la mayoría acude a los módulos presenciales (como sucedió en 2016 y el 2017). Si tomamos el número de personas que utilizaron el SEI en el año 2017 (4,589) podríamos calcular un costo aproximado de alrededor 14 millones de pesos totales y un costo por voto de más de 3 mil pesos por persona (sin desglosar que solamente el 1.58% optaron por esta modalidad de votación remota estrictamente hablando). No es para nada claro que estos números permitan sostener el argumento de la disminución de costos.

Aún con todo esto, algunos Consejeros del IECM sostienen el argumento del ahorro e incluso lo llevan más allá. Sin importar los riesgos que implica, extienden el argumento de su uso contemplando la posibilidad de sustituir, incluso en su totalidad, la modalidad presencial y la postal para contar con elecciones más económicas. [57]

G. Es eficiente y evita el error humano.

El argumento sobre la eficiencia del sistema de VPI señala que la eficiencia aumenta cuando sacamos las elecciones de las manos de las personas y se las entregamos a una computadora. Las limitaciones humanas, dice esta idea, se minimizan hasta desaparecer y el error humano deja de ser un tema, además de que los resultados de las elecciones son más rápidos y precisos de lo que podrían ser a partir de la intervención humana.

57. El Consejero Electoral del IECM Bernardo Monroy señala, por ejemplo, que: "Considerando los costos mencionados, la instalación de cada mesa representó un gasto aproximado de 10 mil pesos (500 USD), que, multiplicado por el número de mesas, dio un resultado de más de 25 millones de pesos (1,250,000 USD) lo que se invierte en una elección "tradicional". En este sentido, si en futuros procesos de participación se sustituyera la votación en papeleta por la de Internet en un 100%, el ahorro sería de gran magnitud, pues, como ya quedó demostrado, la impresión de documentación y material electoral, así como la instalación de MRO representan un gasto que factiblemente puede ser implementado en otras actividades relevantes del proceso electivo", en: Valle Monroy, Bernardo. "México y el voto electrónico en ejercicios de participación ciudadana", *Revista #DDA*, 1 de abril de 2019. Disponible en: https://www.demoamlat.com/mexico-y-el-voto-electronico-en-ejercicios-de-participacion-ciudadana/.

Es cierto que las computadoras significan un avance para la eficiencia en los procesos y la corrección de los errores humanos. Sin embargo, es importante entender que el concepto de eficiencia mide la capacidad de un medio para obtener un fin o, en otras palabras, se evalúa en virtud de la *función que cierto mecanismo realiza*. Si uno supone que los sistemas de voto por Internet realizan solamente y sin excepción lo que nos dicen que realizan, entonces efectivamente el VPI tiene en su favor el elemento de la eficiencia.

El detalle es que eso es precisamente lo que está en entredicho. Primero, porque los sistemas de VPI pueden fallar y muchas veces efectivamente lo hacen. El mejor ejemplo de ello está en la última ocasión que el IECM utilizó su sistema en la Elección de las Comisiones de Participación Comunitaria (COPACO) 2020 y de la Consulta de Presupuesto Participativo 2021. El sistema falló, haciendo que en algunos casos sólo pudieran registrarse entre 2 y 6 votos en varias unidades territoriales (en las alcaldías de Cuauhtémoc y Miguel Hidalgo), **viéndose obligados a usar boletas de papel** para que las personas no perdieran su derecho a votar (aunque en muchos casos las personas desistieron de hacerlo por los tiempos perdidos y la incertidumbre al respecto). [58] Los errores resultaron en impugnaciones ante el Tribunal Electoral y en el reconocimiento por parte del IECM de que las elecciones debían reponerse. [59]

El corolario de este problema es, desde luego, que los sistemas de VPI tienen un grado de complejidad que requiere de una capacitación y profesionalización de los funcionarios que lo operan para que, en casos de

58. Pensando en el punto anterior de los costos, podríamos decir que una elección que fracasa porque las personas no pueden votar y debe ser repuesta es doblemente costosa, tanto por el dinero no efectivo como por el costo de los derechos en juego.

59. En palabras del Consejero Bernardo Valle: "Yo les garantizo a los ciudadanos de estas unidades territoriales, que esas elecciones se van a tener que reponer y que vamos a garantizar que no va haber problemas, junto con las autoridades de seguridad pública de la Ciudad". Ver: La Jornada. "Busca el IECM reponer votaciones en CDMX", 26 de marzo de 2020. Disponible en: https://www.jornada.com.mx/ultimas/capital/2020/03/26/busca-el-iecm-reponer-votaciones-en-cdmx-7759.html; Hoja de Ruta. "Piden explicación sobre falla del sistema electrónico de votación por Internet en elección de Copaco y presupuesto participativo", 23 de marzo de 2020. Disponible en: https://hojaderutadigital.mx/piden-explicacion-sobre-falla-del-sistema-electronico-de-votacion-por-internet-en-eleccion-de-copaco-y-presupuesto-participativo/. En este caso, el Diputado Martín Padilla, Presidente de la Comisión de Participación Ciudadana del órgano legislativo de la CDMX, señaló que el hecho era una "grave falla del sistema" y que además de generar molestia en la ciudadanía, "**generaron un ambiente de desconfianza e incertidumbre de las personas votantes y candidatas sobre los resultados**". En la Parte III del trabajo explicamos en qué consistieron las fallas técnicas y su gravedad ya no sólo en términos de eficiencia sino también de seguridad.

eventualidades, puedan responder a ellas y corregirlas sin poner en riesgo el sistema. En este caso es claro que la previsión y la capacitación fueron insuficientes, al grado de tener que pasar al uso de boletas en papel en un momento en que ya era demasiado tarde para garantizar una jornada electoral exitosa.

Pero además, si demostramos los problemas de seguridad, transparencia y secrecía, entonces la propia función y fin del sistema no puede evaluarse en términos de eficiencia de manera lineal. Por el contrario, debe tomar en cuenta las dificultades de esas dimensiones para medir lo que queremos medir (uno podría decir, para hacer énfasis en esta objeción, que es mucho más eficiente utilizar el sistema de voto por Internet que el de voto presencial si lo que queremos hacer es alterar una elección sin dejar rastros).

La tecnología es una herramienta fundamental para realizar avances y para complementar la acción humana, pero esto no significa que la acción humana deba ser sustituida del todo sólo porque existe la posibilidad de cometer errores humanos. La tecnología no debe sobredimensionar la gravedad de los errores humanos. Durante décadas, las autoridades electorales han desarrollado procedimientos de revisión y observación electoral para el conteo de los votos (así como mecanismos de recuento) en los que participan tanto la sociedad civil como las y los representantes de los distintos partidos políticos. Los errores humanos no son un problema grave en la actualidad, pero los beneficios de contar con esa revisión y observación sí son un respaldo fiable que ayuda a dar legitimidad y credibilidad a las elecciones, aún a pesar de la posibilidad de que los errores existan.

PARTE II / La dimensión normativa del VPI a la luz de sus casos paradigmáticos

El derecho al voto y los procesos electorales tienen ambos elementos normativos; es decir, que cuentan con principios que son valiosos por lo que representan desde un enfoque de los derechos humanos y la democracia. Los principios han sido materializados en las Constituciones, las leyes y las decisiones más importantes de distintos tribunales en la gran mayoría de los países. Cuando hablamos del voto, sabemos que deben cumplirse los principios de secrecía y de libertad ("el voto es libre y secreto", repetimos como mantra electoral de manera cotidiana), así como también el de integridad. Cuando hablamos de las elecciones sabemos que deben cumplir los criterios de publicidad, de transparencia, de certeza, etc. En el fondo, estos principios importan (e importan mucho) porque son indisociables de la legitimidad política de las elecciones.

La legitimidad es la base sobre la que el ejercicio del poder de los gobiernos democráticos se justifica. Un gobierno legítimo refleja el reconocimiento de actuar de acuerdo a los mínimos indispensables que limitan su poder y dan el poder de tomar las decisiones políticas de manera democrática.[60] Las elecciones son, en este sentido, un componente fundamental para determinar cuándo un gobierno es elegido legítimamente (lo que comúnmente se conoce como tener legitimidad política de origen)[61].

En este apartado vamos a revisar tres casos en los que podemos encontrar, por un lado, determinaciones de autoridades estatales que ayudan a delimitar y comprender el alcance de algunos de estos principios y, por otro lado, estudios y análisis concretos que ponen en el centro a los elementos normativos (los principios) del derecho al voto o de las elecciones y que nos dan luz para ver la forma en que estos se relacionan con el nivel técnico de las elecciones que se llevan a través de Internet: Alemania (2009), Estonia (2014) y los Estados Unidos de América -EUA- (2020).

60. Rawls, John. Political Liberalism, New York: Columbia University Press, 1993; Rawls, John, *El derecho de gentes* y *"una revisión de la idea de la razón pública"*, Barcelona, Paidós, 2001, pp. 159-60; Habermas, Jürgen, *Entre naturalismo y religión*, España, Paidós, 2006, pp. 127-28.
61. Sartori, Giovanni. *¿Qué es la democracia?*, Bogotá, Altamir, 1994.

1. Alemania: el Voto Electrónico contra los principios de publicidad y de control ciudadano de la elección

En el año 2009, Alemania desechó el voto electrónico (VE) por considerar que violaba varios de los principios relacionados con el ámbito electoral que eran centrales para su sistema constitucional.[62] La razón principal fue que el *software* utilizado en las máquinas de votación **no podía ser controlado por el público, que no había sido revisado de forma independiente y que el código fuente no era abierto** para su revisión. El tribunal resolvió que para que un mecanismo de votación sea consistente con los principios democráticos que sustentan las elecciones debían respetarse dos principios[63]:

1. **Principio de publicidad.** Todos los pasos esenciales de la elección deben estar sujetos al escrutinio del público; y
2. **Principio de control ciudadano.** Las personas deben poder **controlar y entender** los pasos del acto electoral en lo que corresponde a los aparatos electorales con los que el voto se ejerce, y el resultado del proceso electoral debe poder determinarse de manera fiable **sin la necesidad de tener conocimientos técnicos especiales.**

El tribunal cuestionó la confiabilidad del *software* usado para las máquinas porque no había sido "controlado" por el público. Las auditorías hechas por el gobierno no fueron públicas ni fue posible hacer pruebas de penetración y recompensa independientes, y además el código fuente del *software* no era abierto al escrutinio público.

Las autoridades que defendían el VE argumentaron que: i) la publicidad del acto electoral se garantizaba porque las personas podían imprimir el resultado electoral al votar (con un recibo del voto) y los observadores y la junta electoral podían cotejar los resultados; y ii) que el *Instituto Federal Físico-Técnico* había examinado a detalle la máquina electoral y el *software*, controlándolos junto con las administraciones comunales y las juntas electorales. **Ambos argumentos fueron considerados insuficientes para garantizar los dos principios del proceso electoral.**

El Tribunal fue explícito al decir que los procedimientos para examinar el sistema y su aprobación debían ser públicos y que ningún secreto

62. Tal como mencionamos al principio del trabajo, aunque el VE y el VPI son distintos, sus semejanzas son ideales para evaluar normativa y jurídicamente la forma en que las tecnologías funcionan en el entorno digital y están en tensión con los principios democráticos

63. Sentencia 2 BvC 3/07 - 2 BvC 4/07. Tribunal Constitucional Alemán, 3 de marzo de 2009.

comercial ni interés del fabricante en el uso del *hardware* o *software* podía estar por encima de los principios democráticos de la elección. El principio de publicidad implicaba evaluar el sistema de manera independientemente y, posteriormente, publicar los resultados, porque si esto no se realizaba, la fiscalización del proceso electoral no podía llevarse a cabo.

También estableció que el concepto de auditoría debía entenderse de manera amplia, que no debía limitarse al control hecho por las instituciones públicas ni por los entes designados por ellas para auditar el sistema. Por el contrario, la *comprensión* y *control* del proceso electoral exigía participación del público en la supervisión de los aparatos electorales en las distintas etapas de la elección, no solamente en el momento en que se emitía el voto. Por su relevancia, citamos en extenso la parte central de la sentencia:

> 117[64]
>
> 3. La utilización de aparatos electorales, que pueden registrar el voto electrónicamente y pueden determinar el resultado electoral de manera electrónica, es según ello, sólo compatible con la ley fundamental bajo estrictas condiciones.
>
> 118
>
> a) Al emplear aparatos electorales electrónicos, **debe poderse revisar los pasos esenciales del acto electoral y determinación del resultado de manera confiable y sin conocimientos técnicos especiales.** En última instancia, en vista de la manipulabilidad y la propensión al error de los aparatos electorales electrónicos es que resulta la necesidad de un control de este tipo. En ellos **la recepción de los votos y la contabilización de los resultados electorales se basan en un proceso de cálculo, que desde afuera y para personas sin conocimientos especiales de técnicas informáticas no son comprobables. Por ello es que errores en el *software* de los aparatos electorales son de difícil detección. Además, estos errores pueden afectar no sólo una computadora electoral, sino todos los aparatos utilizados. Mientras que en las elecciones tradicionales con boletas electorales las manipulaciones y falsificaciones electorales bajo las condiciones marco de las prescripciones vigentes, a los que pertenecen también las reglas sobre publicidad, resultan poco posibles –o de cualquier manera sólo con un esfuerzo considerable y un riesgo de descubrimiento muy alto y de efecto preventivo-, intervenciones en los aparatos electorales dirigidos electrónicamente pueden, en principio, con un esfuerzo relativamente escaso, obtener un alto impacto.** Incluso manipulaciones en un sólo aparato electoral puede influenciar no sólo votos individuales, sino todos los votos que fueron dados con ayuda de este aparato. Más grande es el alcance del error electoral que se ocasionan con las modificaciones y mal funcionamiento de un solo *software* que se extiende a todos los aparatos. El efecto de gran alcance de los posibles

64. Todos los énfasis en el texto de la sentencia son añadidos nuestros.

errores de los aparatos electorales o las falsificaciones electorales mandan la realización de medidas precautorias especiales para proteger el principio de publicidad de la elección.

119

aa) El elector debe –también sin conocimientos detallados de computación- poder comprender si su voto es registrado como base del escrutinio o –si los votos primero se escrutan con apoyo técnico- de cualquier manera, como base de un posterior recuento registrado verdaderamente. **No alcanza una remisión a que confíe en ello, sin la posibilidad de examinar por sí mismo el funcionamiento correcto del sistema. De allí que no alcance, si sólo es informado exclusivamente por un indicador electrónico de que su voto ha sido registrado. Eso no le posibilita un control suficiente por el elector. La misma comprensión también debe estar dada para los órganos electorales y los ciudadanos interesados.**

120

De ello resulta, que los votos no pueden quedar depositados exclusivamente en una memoria electrónica. **El votante no puede ser remitido, luego de la votación electrónica, a confiar exclusivamente en la integridad técnica del sistema.** Si el resultado electoral se obtiene por medio de la elaboración guiada por ordenador de los votos depositados en la memoria electrónica, no alcanza, si sólo se puede tomar conocimiento mediante un resumen impreso en papel o de un indicador electrónico. Porque de esta manera, electores y órganos electorales sólo pueden examinar si el aparato electoral ha procesado tantos votos como electores han sido autorizados a emplear ese aparato electoral. **En estos casos no es reconocible fácilmente, si ha habido errores en la programación del *software* o de falsificaciones electorales intencionales por medio de la manipulación del *software.***

[...]

122

En todo caso debe quedar asegurado, **que el elector domina su emisión del voto y los órganos electorales y ciudadanos interesados pueden verificar fiablemente el resultado electoral sin previos conocimientos técnicos especiales.** No es necesaria aquí una decisión acerca de si existe alguna otra posibilidad técnica que permita una confianza en la corrección del proceso de determinación electoral basada en la comprensión, y que con ella se baste al principio de publicidad de la elección.

[...]

123

b) Las limitaciones a la controlabilidad ciudadana del proceso electoral no pueden ser compensadas con que los aparatos de muestra sean controlados en el marco del Procedimiento del Permiso de Versión, o que los aparatos utilizados concretamente en la elección sean controlados previamente por una institución oficial sobre su concordancia con determinadas exigencias de seguridad y su integridad técnica. **El control de los pasos esenciales de la elección fomenta una confianza fundada en el debido orden de la elección sólo en la manera exigida, de que el ciudadano pueda comprender fiablemente el proceso electoral por sí mismo.**

124

Por este motivo un amplio conjunto de otras medidas de seguridad (Por ejemplo, controles sobre la consigna de aparatos electorales, poder comparar los aparatos utilizados en cualquier momento con un modelo examinado oficialmente, punibilidad de fraudes electorales y organización descentralizada de la elección) tampoco son adecuados por sí mismos, para **compensar la falta de controlabilidad de los pasos esenciales del proceso electoral por parte de los ciudadanos.**

125

Por consiguiente, ni una participación del público interesado en el proceso de evaluación o del permiso de aparatos electorales, ni la publicación de los informes de evaluación o caracteres de construcción (incluyendo los códigos fuente del *software* en el caso de aparatos electorales guiados por ordenador) contribuyen decisivamente en asegurar el nivel exigido constitucionalmente de controlabilidad y comprensión del proceso electoral. Los exámenes técnicos y procesos oficiales de permiso, que de todas maneras sólo pueden ser apreciados con pericia por especialistas interesados, se refieren a un estado del proceso que se encuentra alejado del de la emisión del voto. La participación del público necesita por ello, para lograr la exigida supervisión fiable, medidas complementarias ulteriores.

Vale la pena detenerse paso a paso en el razonamiento del tribunal constitucional. Primero, en que los jueces ponen en el centro de su razonamiento a la población en general y su posibilidad de *entender* y *confiar* en el proceso electoral **sin necesidad de tener conocimientos técnicos.** Las tecnologías de voto electrónico dificultan esta comprensión y requieren conocimientos técnicos para entender cómo funcionan los dispositivos (el *hardware*) y el sistema propiamente dicho (el *software*).

Un segundo elemento que subrayan es el de la *dificultad de detectar los errores o manipulaciones de los sistemas de voto electrónico* y el riesgo que esto implica. Como el sistema de votación está centralizado por un programa, si este llega a ser comprometido, toda una elección puede ser afectada a partir de ahí y poner en riesgo toda una elección.[65]

El tercer punto es que no basta con el argumento de que podemos confiar en la tecnología que respalda el sistema de voto electrónico, sino que la ciudadanía debe poder examinar "por sí misma el funcionamiento correcto del sistema [...] De allí que no alcance si sólo es informado

65. El riesgo de la manipulación completa de una elección por la centralización del sistema tecnológico es un rasgo compartido entre el VE y el VPI (aunque en este último los riesgos de sus vulnerabilidades se agravan). Como veremos en el análisis del caso de Estonia, tomar control del sistema vuelve más asequible la manipulación de una elección: "El peligro de votar así es que la manipulación de una elección, debido al poder de la informatización, puede ser a una escala mucho mayor con una conspiración muy pequeña, y también muy difícil de detectar", en Halderman, Alex J. *Security Analysis... op. cit.*

exclusivamente por un indicador electrónico que su voto ha sido registrado. Eso no le posibilita un control suficiente por el elector" (párrafo 119 aa y 120).

Resultado de este razonamiento, el cuarto punto es que la v*erificabilidad de los resultados* debe poder realizarse también sin conocimientos técnicos (para que quede dentro del control ciudadano), de acuerdo a la lógica del principio de "publicidad" de la elección, y siempre "por sí mismo". No es suficiente, otra vez, confiar en un sistema que supuestamente hace lo que dice que hace (párrafos 122 y 123b).

En quinto lugar, el órgano judicial considera que las medidas de seguridad complementarias dentro de un sistema que no puede comprenderse ni auditarse por la ciudadanía no son suficientes "para compensar la falta de controlabilidad de los pasos esenciales del proceso electoral por parte de los ciudadanos" (párrafo 124). Por ello concluye que ni la participación del público interesado en la evaluación del sistema, ni la publicación de los informes de evaluación del mismo logran satisfacer el estándar constitucional de controlabilidad y comprensión del sistema electoral (párrafo 125).

El Tribunal Constitucional Alemán estableció que los principios de transparencia y publicidad sobre el código de las computadoras que permiten el procesamiento de resultados y el desarrollo del sistema de voto electrónico, debían ser abiertos y auditables de forma independiente. Sin la auditabilidad total del sistema, la integridad del proceso electoral quedaba comprometida; sin la evaluación de todos los elementos del sistema en todas las etapas, la integridad del voto se perdía.[66]

66. Otro caso paradigmático relacionado con este punto es el de Holanda en el 2006 (también sucedió en Brasil y en Irlanda en el 2009). Un colectivo pudo exponer que utilizando cierta tecnología (por medio de la interferencia de señales Van Eck) podían ver lo que pasaba en la pantalla de la computadora para literalmente ver por quién se votaba (esto era posible incluso a muchos metros de distancia de la casilla de votación por Internet centralizada). En el caso de Holanda, el colectivo *We don't trust voting computers* realizó demostraciones públicas donde mostraban cómo las computadoras podían ser hackeadas a distancias de 30 metros, rompiendo con el principio de la secrecía del voto. Al respecto ver: Herald Tribune. "Dutch government scraps plans to use voting computers in 35 cities including Amsterdam", The Associated Press, October 30, 2006. Disponible en: https://web.archive.org/web/20061119103008/http://www.iht.com/articles/ap/2006/10/30/europe/EU_GEN_Netherlands_Voting_Machines.php. Para el mismo caso pero en Brasil en el 2009: IDGNOW. Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil, 20 de novembro 2009. Disponible en: https://web.archive.org/web/20120601054809/http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/; y: techdirt. "Brazil E-Voting Machines Not Hacked... But Van Eck Phreaking Allowed Hacker To Record Votes, november 23, 2009. Disponible en: https://www.techdirt.com/articles/20091123/0147047048.shtml. Sucedió lo mismo en el sistema de votación en Irlanda, donde el proyecto al final fue abandonado definitivamente. Al respecto ver: RTE. "Report raises e-voting equipment concerns", December 8, 2002. Disponible en: https://www.rte.ie/news/2002/1208/32905-voting.

Si bien el Tribunal Constitucional Alemán no señaló que todo tipo de tecnología era incompatible con el voto y con las elecciones, sí dijo que este tipo de sistema no cumplía con los requisitos mínimos indispensables para que las votaciones se realizaran de acuerdo a los principios democráticos. A partir de esta decisión, Alemania no volvió a intentar usar el voto electrónico ni ninguna otra modalidad de voto por Internet.

2. Estonia: los riesgos de seguridad del Voto por Internet contra los principios de secrecía e integridad del voto

Estonia es el referente del voto por Internet a nivel mundial, no sólo porque lleva usándolo desde hace casi dos décadas sino porque lo utilizan en las elecciones nacionales de manera regular. El largo recorrido y las numerosas experiencias lo vuelven el caso paradigmático para estudiar el VPI porque cuenta con numerosas investigaciones sobre los resultados y el funcionamiento del sistema de votación, al mismo tiempo que tiene un largo registro de las respuestas del gobierno cuando los estudios han cuestionado el uso de este sistema. Estonia lleva ocho elecciones con VPI y en ocasiones ha tenido más del 30% de la votación total por esta vía.

El punto de quiebre en la experiencia estonia sobre el VPI tuvo lugar en el año 2014, cuando un grupo de expertos internacionales invitado por el propio gobierno pudo revisar, por primera vez en la historia de su implementación, el sistema de manera detallada (aunque con algunas limitaciones que explicamos más adelante). Aunque existía un análisis anterior (del año 2011) que había señalado una cantidad enorme de problemas y riesgos del sistema, en ese caso no había tenido acceso al código fuente del *software* en su totalidad.[67]

Tras publicarse el informe del 2011 que señalaba un alto riesgo de que el sistema hubiera sido *hackeado*, los resultados electorales fueron impugnados ante la Comisión Nacional Electoral (CNE), quien rechazó la apelación por considerar que se habían tomado las previsiones necesarias para detectar intentos de *hackear* la elección y manipular los votos, sin especificar cuáles habían sido ni en qué consistían, ni mostrar cómo habían

67. Halderman, Alex J. *Security Analysis... op. cit.*

funcionado. Finalmente, el caso llegó a la Corte Suprema, quien revisó la apelación hecha por un ciudadano, pero la desechó por considerar que no se habían violado sus derechos.

El análisis se apoyaba en un estudio anterior realizado por la Organización para la Seguridad y la Cooperación en Europa y la Oficina de Instituciones democráticas y Derechos Humanos (OSCE/ODIHR por sus siglas en inglés), que determinó que el sistema era inseguro por seis razones: i) la privacidad de los votantes (el voto secreto) era vulnerable; ii) las computadoras de las votantes eran vulnerables a *malwares*; iii) existía una amenaza interna (*insider threat*); iv) los servidores eran vulnerables; v) el sistema no era abierto ni transparente; y vi) no se había llevado una evaluación de seguridad del sistema por expertos independientes en seguridad computacional. El gobierno descansaba en una confianza injustificada sobre la seguridad y protección del sistema.[68] De ambos informes, el de 2011 y el de 2014, los riesgos pueden resumirse en los siguientes puntos.

El primer problema para la secrecía del voto se da cuando el sistema de Internet separa la identidad del votante del sentido de su voto, lo que se conoce como proceso de anonimización y que se lleva a cabo por programas criptográficos que tienen un sistema "mixnet" que alterna los votos una vez separados (el proceso es realizado por un programa elaborado por un técnico que lo hace correr). Pero ¿Qué contiene ese programa? ¿Cómo podemos verificar que no haya otra copia de las boletas con sus nombres asociados en otro lugar del mismo? Esta segunda pregunta es particularmente importante porque un respaldo en este sentido debería existir ante el riesgo de la pérdida de la información.

Todo proceso de anonimización sigue una metodología similar a esta: i) se corre el programa que separa los nombres de los votantes de las boletas electrónicas y se crean dos archivos (nombres y boletas-votos sin nombre); ii) se alternan o revuelven los archivos en forma aleatoria para anular cualquier orden o correlación entre los nombres y los votos; iii) se revisa que ningún dato se haya perdido o corrompido; iv) se hacen respaldos en archivos separados; y v) se destruyen todas las copias y

68. Simmons, Barbara. *Report on the Estonian Internet Voting System*, 3 de septiembre del 2011. Disponible en: https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/. El informe de la OSCE: *Estonia, Parliamentary Elections, 6 March 2011: Final Report, 6 March 2011* puede consultarse en: https://www.osce.org/odihr/77557.

respaldos de las boletas que tienen un nombre asociado a ellas. El problema está en ese último paso, porque es inherentemente inverificable:

> "No hay forma de probar que esas copias fueron destruidas; de cualquier modo sería muy difícil encontrar TODAS las copias normalmente hechas en el curso rutinario del comportamiento del sistema que, como un asunto práctico, probablemente no se logre hacer por completo. No podemos ver si no quedó nada de data en algún lugar, que permita luego la reconstrucción y la asociación porque, inherentemente, la privacidad del voto no puede auditarse ni observarse de manera adecuada".[69]

El problema es resultado del dilema que señalamos más arriba: la inevitable tensión entre la integridad de las elecciones y la secrecía del voto. **La integridad** consiste en que el resultado de una votación corresponde con lo que los votantes expresaron en las urnas; es decir, que los resultados coinciden con sus intenciones: los votos deben ser emitidos según la intención del votante y luego deben ser contados tal como fueron emitidos. **La secrecía** implica que las personas no develen su intención electoral; que una vez votado no puedan mostrar por quién votaron aún cuando quieran.

Ambos elementos están en tensión porque las medidas tradicionales que fortalecen la integridad, tal como dar un recibo (como se hace en el comercio electrónico o al extraer dinero de una cuenta), implican que la secrecía se ponga en juego, mientras que las medidas que fortalecen el secreto del voto (como el *mixing*) llevan a la gran dificultad (incluso la imposibilidad) de poder asegurar la integridad de la elección porque al fortalecer la secrecía se dificulta saber si un voto fue manipulado o no.[70]

El segundo problema relacionado a la seguridad nos lleva al argumento clásico de las transacciones bancarias en Internet. El informe de Simmons muestra que existen *malwares* que han permitido el robo de muchísimo dinero en línea al romper la seguridad de los bancos. Se trata de algo común y que sigue pasando todo el tiempo en todo el mundo. En la auditoría se mostró que una adaptación de un virus llamado "Zeus" podía ser conseguido de forma relativamente sencilla para robar la elección. Este problema combina la simpleza de la cotidianeidad humana con la complejidad tecnológica. Limpaa Helger (experta en criptografía) lo explica diciendo que:

69. Simmons, Bárbara. *Report on the Estonian Internet... op. cit.*
70. Halderman, Alex J. *Security Analysis... op. cit.*

> Las computadoras para votar tienen un problema obvio: la mayoría de la gente es iletrada computacional y no es capaz de revisar si sus computadoras están infectadas. Aún si tienen el antivirus más nuevo (de lo que no podemos estar seguros), ese antivirus puede no ser suficiente por sí mismo para detectar un nuevo *malware* hecho específicamente para *esa* elección y lanzado justo antes de ella [...] Ese *malware* podría hacer mucho daño, tal como interceptar la conexión entre tú y tu ID (básicamente dejando que la ID firme los votos incorrectos), entre el FUI y lo que en verdad sucede dentro de la computadora, etc.[71]

Los dispositivos de las personas son vulnerables y la corrección de estas vulnerabilidades es un trabajo permanente que requiere una actualización constante de los sistemas de operación y de seguridad. Como mencionamos más arriba, ninguna computadora, ningún teléfono inteligente es *inhackeable*. Desde el FBI, pasando por grandes compañías como Google y hasta la CIA, la constante advertencia y la experiencia muestran que incluso los sistemas más sofisticados de seguridad pueden ser y son vulnerados.

El tercer problema relacionado con la seguridad es el de la transparencia y la falta de auditorías independientes. En la elección del 2011, las auditorías que el gobierno realizó de su sistema no fueron públicas y solamente se entregaron a la CNE y a ciertos observadores seleccionados por el gobierno. La evaluación de seguridad, además, no estaba abierta a expertos internacionales independientes y quien quisiera revisar el código debía firmar un acuerdo de confidencialidad muy exigente, que garantizaba que el sistema quedara blindado de la observación externa al gobierno.[72]

De cara a las elecciones del 2015, con la visita de expertos internacionales independientes y la novedad de permitir la revisión del código del sistema por primera vez, liberaron el código del servidor aunque dejaron el código del cliente cerrado.[73] El sistema de VPI funcionaba de la siguiente manera:

1. Una vez que la electora votaba, su boleta se encriptaba (con un algoritmo RSA) para luego hacer un *padding* aleatorio;

2. Se hacía una firma digital utilizando la credencial ID que tiene toda la ciudadanía en Estonia;

71. Helger, Lipmaa. *Paper-voted (and why I did so),* March 5 2011. Disponible en: https://helger.wordpress.com/2011/03/05/paper-voted-and-why-i-did-so/.
72. Simmons, Bárbara. *Report on the Estonian Internet... op. cit.*
73. Springall, Drew; Finkenauer, Travis; Durumeric, Zakir; Kitcat, Jason; Hursti, Harri; MacAlpine, Margaret and J. Alex Halderman. *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS '14), November 2014. Disponible en: https://estoniaevoting.org/findings/paper.

3. Se enviaba la boleta electrónica firmada al servidor de las elecciones, donde se almacenaba hasta llegado el momento de contar los votos;

4. Las electoras podían verificar su voto con un código QR que tenía: i) un identificador de boleta y ii) los valores aleatorios que se hicieron al encriptar el voto. A su vez, el elector podía cambiar y reemplazar su voto las veces que quisiera hasta antes de cerrar la elección (como medida de protección contra la coerción).

5. El proceso de conteo era similar al conteo de los votos postales: los servidores toman las boletas almacenadas y les remueven las firmas para luego ponerlas en un DVD que llevan a un servidor de conteo que está sin conexión a Internet y que tiene la llave privada para desencriptar las boletas. El contador ve los votos pero no ven las firmas, teniendo el resultado sin violar los nombres y sin (supuestamente) romper la secrecía.

En concreto, el estudio del 2014 encontró distintas amenazas a la seguridad que consideró severas. Una tenía que ver con los riesgos del lado de los votantes y la otra con los riesgos del sistema. Un votante podía ser engañado e infectado con un *malware* para hacerle creer que usaba el sistema de manera normal cuando no era así. Al tomar control del dispositivo de una persona era posible utilizar su código fuente para realizar ingeniería inversa y reconstruir toda la elección (este ejercicio fue realizado y demostrado por los investigadores). Ganar control del dispositivo permitía: espiar el proceso de elección del votante, robar su clave mientras la escribía para después, cuando el votante utilizara su ID en otra acción cualquiera (por ejemplo, para usar su banco online), utilizar esa clave robada para emitir el voto de reemplazo en la *App* para votar sin que el votante se diera cuenta.[74]

Otro punto señalado fue que los votantes utilizan su propia computadora o dispositivo en su casa o, supuestamente, en el lugar donde estarían más cómodos. Aunque intuitivamente esto pareciera favorable, esa característica implicaba la ausencia de contar con un entorno protegido en el que se garantiza que la persona está protegida y libre de coerción; un lugar donde su nombre de usuario y contraseña no pueden ser robados.

74. Halderman, Alex J. *Security Analysis... op. cit*. La infección de dispositivos vía las apps de votación puede hacerse de varias formas: con un ejército de bots infectando masivamente computadoras, con ataques 0-day en alguna app popular donde haya muchos posibles votantes, o metiendo códigos maliciosos dentro de la aplicación de votación que se va a usar. El proceso de verificación también puede ser vulnerado porque los sistemas pueden ser atacados por *apps* maliciosas para comprometer la *app* del votante ya que por la convergencia de plataformas pueden atacarse ambos aspectos simultáneamente.

El talón de aquiles del sistema estaba, sin embargo, en los servidores, por ser el lugar donde los votos se desencriptan sin que nadie los vea para luego mostrar los resultados del conteo de votos.[75] La clave para entender el riesgo es la siguiente: para tener un sistema seguro, necesitamos de otro sistema que lo haga seguro. Esto genera un mecanismo en cadena que eventualmente hace depender la seguridad del sistema como un todo de alguna parte que puede ser vulnerable. No sólo se trata del riesgo de corrupción interna de funcionarios que puedan infectar un elemento que permita tomar control, sino que los dispositivos de *hardware* y de *software* con los que un sistema funciona requieren de sujetos externos a las autoridades electorales que los manipulan para hacer funcionar el sistema, y de puntos donde un atacante puede ganar acceso eventualmente.[76]

El sistema de VPI requería de un DVD de instalación que descargaba una copia del programa que corría en las elecciones. Este programa se descargaba a su vez desde otro servidor que sí estaba conectado a Internet (lo que se llama un servidor de desarrollo). De este modo se mostró que ese servidor podía infectarse para luego infectar el DVD y comprometerlo para instalar un código de puerta trasera (*backdoor*) en el servidor de conteo, en el momento en que se montaba. Una vez realizado el ataque, cambiar los votos era relativamente fácil. En el ejercicio se mostró que a partir de aquí era sencillo grabar votos fraudulentamente y luego encriptarlos en el DVD a través del servidor de desarrollo.

Todas y todos los especialistas concluyeron que las vulnerabilidades de seguridad eran serias y que estas se agravaban frente al supuesto de que un sujeto con "poder estatal" (o similar) estuviera interesado de explotarlas. Las elecciones en este sentido podían convertirse en una situación de Seguridad Nacional frente a amenazas de carácter internacional.[77]

75. Los sistemas de encriptación no logran por sí mismos resolver los riesgos de *malware* en los dispositivos de los usuarios ni sus riesgos de seguridad. Como los votos y la elección pueden ser manipulados antes del proceso de encriptación, no sabemos qué es lo que pasa tras bambalinas y estamos obligados a confiar en lo que nos dicen. Perdemos el elemento de saber que nuestro voto fue "emitido como deseaba" (*cast as intended*), "contado como lo emití" (*counted as cast*) y que "todos los votos fueron contados como fueron emitidos" (*al votes counted as cast*).

76. La programación de los servidores, por ejemplo, obliga a que en algún momento deban de conectarse a Internet para poder montar el sistema de votación. Todas las situaciones similares se convierten en una vulnerabilidad de este tipo.

77. En el siguiente caso de estudio, de los EUA, veremos cómo a partir de este problema el gobierno estadounidense ha catalogado a la infraestructura especializada para llevar a cabo elecciones electrónicas como "infraestructura crítica", considerada fundamental para la Seguridad Nacional.

3. Estados Unidos de América: la Seguridad Nacional y el rechazo Federal al Voto por Internet

El caso de Estados Unidos es el más reciente e ilustrativo del Voto por Internet. En el contexto de la pandemia causada por el COVID-19, varios de los gobiernos locales empezaron a barajar la posibilidad de utilizar el VPI. La posibilidad fue analizada a profundidad tanto por agencias de gobierno como por especialistas en la materia, ante la preocupación por las vulnerabilidades en materia de seguridad.

La historia del VPI en este país tenía un antecedente importante en el que se habían demostrado las debilidades del sistema que pretendía usarse en Washington D.C., a finales del año 2010. Las autoridades en ese caso habían invitado a cualquier especialista a evaluar su sistema porque consideraban que era totalmente seguro, por lo que dejaron el código abierto para probar su punto, toda una semana antes de las elecciones. La idea era que el sistema fuera puesto a prueba a través de un *hackeo* ético y así demostrar que era seguro e incentivar su uso.

Un grupo de especialistas estudió el código y encontró un error que no sólo les permitió tomar el control total del sistema y robar los votos para cambiarlos (de hecho modificaron la boleta electrónica para votar por personajes de robots asesinos o figuras de inteligencia artificial, sólo para que llegado el momento de ver los votos, las autoridades se dieran cuenta de que habían sido *hackeadas*), sino que lograron manipular el código para dejar una pista del fraude a las autoridades para ver si sus sistemas de seguridad les permitían detectar violaciones de seguridad. La pista era una canción de la banda de guerra de la Universidad de Wisconsin (lugar donde investigaba el equipo) que tocaba al final del proceso de votación (cuando el sistema agradecía por haber emitido el voto por Internet). Las autoridades no se dieron cuenta hasta tres días después, cuando un usuario les llamó para decirles acerca de la canción y preguntar por qué razón la habían puesto.[78]

El *hackeo* fue a través del proceso de encriptación, que permitía que la boleta electrónica fuera secreta hasta pasar a otra máquina para desencriptarla. Además pudieron *hackear* el sistema de cámaras de ciertos centros

78. Halderman, Alex J. *Security Analysis... op cit*

de votación en donde pudieron ver la labor de los oficiales. Finalmente atacaron las vulnerabilidades, robando los votos, reemplazando esos votos con los suyos y estableciendo "puertas traseras" para saber cuando entraba algún voto y así ver la intención del mismo, y después limpiaron todos los rastros cuando ya tenían el control del sistema. El gobierno desistió de utilizar el VPI y, en su lugar, permitieron a los votantes en el exterior imprimir una boleta en papel que ellos les enviaban y después enviarla por correo.[79]

EUA tiene una larga historia del uso de voto electrónico en sus elecciones locales, en particular para electores integrantes de las fuerzas militares que se encuentran fuera del país y para personas con discapacidad. Con las propuestas realizadas ante la pandemia, e impulsadas fuertemente por los intereses de varias empresas que se encargan de desarrollar *software* y *hardware* para realizar elecciones por Internet, distintas agencias de gobierno advirtieron a los Estados que el VPI implicaba riesgos altos de ciberseguridad y vulnerabilidades. La práctica podría comprometer por completo las elecciones, a diferencia de la alternativa de utilizar boletas de papel por correo. El memorándum estableció que los ataques al VPI: "pueden conducirse desde cualquier lugar del mundo, en grandes cantidades, y comprometer la confidencialidad y la integridad del voto y/o detener su disponibilidad".[80]

Las empresas que se benefician desarrollando sistemas de voto por Internet rechazaron las acusaciones. La principal empresa encargada de impulsar el VPI en el contexto de la pandemia es "Voatz", quien declaró que su sistema de seguridad era completamente seguro y podía responder a todas las amenazas de seguridad que existían en la actualidad. Frente a estas declaraciones, el MIT realizó un informe en el que avisó sobre un número importante de fallas de seguridad de su sistema.

El estudio fue claro sobre la necesidad de transparencia en el diseño de los sistemas de votación por Internet y demostró que el sistema podía ser *hackeado* para revelar el voto de una persona, y que si el servidor era vulnerado los votos podían alterarse fácilmente. También reveló

79. *Idem.*
80. FBI (Federal Bureau of Investigations)... *op. cit.; The Wall Street Journal. Agencies Warn States that Internet Voting Poses Widespread Security Risks,* by Dustin Volz. May 8, 2020. Disponible en: https://www.wsj.com/articles/agencies-warn-states-that-internet-voting-poses-widespread-security-risks-11588975848.

preocupaciones en torno a la privacidad y la exposición de los datos personales, ya que si el sistema se *hackeaba*, la persona con el control accedería a la fotografía, la identificación y otros datos personales importantes de los votantes.

> "No podemos experimentar con nuestra democracia. El consenso de los expertos en seguridad es que realizar una elección segura por Internet no es posible en la actualidad. [...] El razonamiento es que la larga cadena de vulnerabilidades existentes puede dar a un adversario una influencia indebida sobre una elección, y el *software* existente hoy es suficientemente débil para afirmar que la existencia de fallas desconocidas es un riesgo demasiado grande para tomar" [Traducción nuestra].[81]

Sin embargo, la empresa rechazó categóricamente los señalamientos del MIT y dijo que abriría su sistema y el código de su App de votación para que fuera revisado por un grupo independiente de expertos. Así que el nuevo estudio tuvo lugar. El estudio encontró 79 casos de vulnerabilidades, de los cuales un tercio fueron consideradas de alta gravedad y, además, confirmó los señalamientos realizados previamente por el MIT. Uno de los principales problemas era que la forma de recopilar la información de las y los votantes rompía con su anonimato porque el servidor recopilaba los datos de manera que si el sistema se hackeaba era simple vincular los nombres con las intenciones de voto.[82]

El sistema que *Voatz* entregó para hacer el estudio independiente tenía más de 168 mil líneas de fuente pura de código, que estaban en alrededor de 2 mil 100 documentos y no constituía el sistema completo (reportado como altamente complejo). Un tercio de los problemas de seguridad de "alta gravedad" correspondían a las siguientes categorías: i) criptografía: problemas con los algoritmos y los protocolos criptográficos; ii) exposición de datos: problemas con información sensible de los desarrolladores de Voatz que podía ser filtrada a atacantes; iii) validación de datos: la confianza del sistema en datos no validados otorgados por los clientes; iv) el *logging de la auditabilidad y los controles de responsabilidad:* la incapacidad de rastrear comandos dados por los administradores; v) *asesoramiento de la*

81. Specter, Michael; Koppel, James & Weitzner, Daniel. *The Ballot is Busted... op cit.* Para la nota del MIT al respecto ver: MIT News Office. *MIT researchers identify security vulnerabilities in voting app,* February 13, 2020. Disponible en: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.
82. Trail of Bits. Full Report on the Voatz Mobile Voting Platform. March 13, 2020. Disponible en: https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/.

seguridad y autorización de controles: un monitoreo continuo insuficiente. procedimientos documentados y conexiones documentadas; vi) *controles de manejo de la configuración:* falta de configuraciones base y análisis de impacto de la seguridad; vii) *planes de contingencia:* planes insuficientes en caso de desastre y para la continuidad del servicio; y viii) *respuesta insuficiente a incidentes,* mantenimiento y evaluación de riesgo en los planes y protocolos.[83]

Los expertos de Trail of Bits concluyeron que, aún cuando el análisis del complejo sistema era parcial, la cantidad de vulnerabilidades mostraba que era inseguro y que probablemente existían otros problemas relacionados que no podían ser determinados en el estudio. Su estudio, junto con el del MIT y el pronunciamiento conjunto de las agencias gubernamentales, hizo que varios de los Estados que buscaban implementar el VPI (tal como West Virginia) se retractaran y cancelaran su implementación. Sobre esa decisión:

> Hay algunas preguntas difíciles sobre qué hacer con todo esto, pero una es sorprendentemente clara: necesitamos dejar los sistemas de votación tan lejos de Internet como sea posible. Hay un consenso creciente y claro en este punto. Las guías federales sobre las nuevas máquinas de votación tal vez pronto prohibirán que los sistemas de votación se conecten a Internet o incluso que usen Bluetooth.[84]

4. Elementos normativos y principios democráticos de las elecciones: de cara a un modelo que garantice el derecho a votar

Las experiencias analizadas nos permiten tomar los elementos normativos constituyentes del derecho al voto y los principios rectores de las elecciones que se enmarcan en la discusión sobre el voto por Internet. Los elementos y los principios nos servirán como base para proponer un modelo en el caso

83. El reporte de Trail of Bits sobre el sistema de VPI y sus vulnerabilidades puede revisarse en: https://github.com/trailofbits/publications/blob/master/reviews/voatz-securityreview.pdf.
84. Goodman, Rachel y Halderman, Alex J. "Internet Voting is Happening Now. And it could destroy our elections", 15 de enero de 2020. Disponible en Slate: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html. En el mismo sentido: "Al final, los problemas de Voatz no son sorprendentes: votar en línea es uno de los problemas de seguridad más difíciles. En mi opinión, tardará al menos una década -si es que algún día llega a pasar- antes de que podamos votar en línea de manera segura en elecciones generales, y llegar ahí necesitará de un gran progreso en el campo de la seguridad" [Traducción nuestra], en: https://threadreaderapp.com/thread/1238494514299277318.html, 13 de marzo de 2020.

mexicano que sea, primero, acorde al marco constitucional e internacional y, segundo, que logre incorporar las características más salientes de esa estructura normativa en el contexto de las nuevas tecnologías y de Internet. Con un modelo integrado contaremos con criterios para evaluar las experiencias del VPI en el caso mexicano, así como su compatibilidad con los principios democráticos y los derechos que la democracia defiende en el ámbito electoral.

El set de principios que proponemos como modelo en el apartado siguiente se apoya en el análisis contextual y comparado de las experiencias principales y más ilustrativas del VPI, que nos permiten entender tanto las particularidades técnicas (y sus problemas de seguridad, secrecía e integridad) como los dilemas jurídicos del funcionamiento cotidiano de las elecciones en Internet. Partiendo de Alemania, Estonia y EUA, podemos tender un puente que conecte con el marco constitucional mexicano e internacional para revisar el ejemplo más desarrollado de voto por Internet en México, el del IECM en la capital del país.

Esquemáticamente, la experiencia comparada nos muestra que los principios involucrados en una elección por Internet son: i) la publicidad y la transparencia de la elección; ii) el control ciudadano; iii) el secreto del voto; y iv) la integridad y la seguridad del voto y de las elecciones. Estos pueden integrarse analíticamente de la siguiente manera.

i) Publicidad, transparencia y control ciudadano

La experiencia del Tribunal Constitucional Alemán sirve para tomar dos principios fundamentales en la organización y la operación de las elecciones. **La publicidad y el control ciudadano** apuntan a la importancia de poder ver los pasos esenciales del proceso electoral y de poder entender en qué consisten, tanto las etapas como los resultados, **sin la necesidad de tener conocimientos técnicos especiales.** La democracia debe ser un sistema de gobierno comprensible para todas las personas, en el que las acciones que pueden ser escrutadas y asimiladas por los sujetos que conforman la comunidad política.

La transparencia de una elección por Internet depende de que pueda ser evaluada de forma independiente y completa (y no revisada parcial y sectorizadamente). Las experiencias de Estonia y de los Estados Unidos de América nos sirven para entender la relevancia de contar con auditorías expertas independientes que tengan la posibilidad de **revisar en su totalidad el código del sistema y las aplicaciones con las que se utiliza,** además de la necesidad de **publicar posteriormente los hallazgos de la revisión para que la ciudadanía pueda, primero entenderlos, y después cuestionarlos sin que la información quede reservada para las autoridades.**

Con el estado actual que la tecnología (sus particularidades técnicas y la complejidad que los sistemas computacionales), la criptografía y la programación tienen en la actualidad, parece imposible "ciudadanizar" el funcionamiento de los sistemas de voto por Internet, al menos por dos razones: a) porque la práctica de los países que utilizan el VPI es cerrada al público, muy poco transparente y casi hermética a las revisiones expertas e independientes; y b) porque los sistemas de VPI funcionan de manera que el entendimiento del sistema requiere un conocimiento altamente especializado, al que sólo algunas personas con profundo saber técnico y mucho interés pueden acceder sin complicaciones. La hiperespecialización del conocimiento es muy poco democrática y saca la comprensión de las elecciones de las manos de las personas para dársela a una élite minoritaria.

Suponiendo que la democratización del conocimiento especializado fuera posible, los principios de publicidad y control implican una **obligación de apertura y evaluación del sistema de VPI** para todas las autoridades que quisieran hacer uso de él. Si el código del sistema es cerrado, si las aplicaciones, *hardware* y *software* sólo pueden ser evaluadas parcialmente o por quienes son seleccionados (y pagados) por las autoridades, entonces es imposible convencernos -a menos que lo hagamos como un acto de fe- de que el sistema de VPI funciona y cumple con lo que promete.

ii) La integridad y la secrecía del voto

Las experiencias de Estonia y de EUA también nos sirven para comprender qué dimensiones de la secrecía y de la integridad están en juego cuando

hablamos de votar por Internet. En primer lugar, sabemos que la tensión entre ambos principios (el dilema integridad-secrecía) hace muy difícil (si no imposible, al menos en la actualidad) satisfacerlos en el grado que exigen porque tiran en direcciones contrarias. Como los mecanismos de anonimización y aleatorización del voto (que buscan evitar que la secrecía se rompa) hacen casi imposible saber si una elección fue *hackead*a, el sistema nos obliga a confiar ciegamente en que su seguridad es absoluta y, si no lo es y falla, no es posible saber si los votos fueron manipulados.

A diferencia de los sistemas bancarios por Internet, que privilegian la seguridad de las operaciones porque no existe un requisito de secrecía (en el sentido en que existe en el derecho al voto) y porque vinculan la seguridad con la identidad de las personas al realizar cualquier operación (su sistema funciona porque en todo momento se sabe quién hizo qué, a diferencia del VPI en el que el paradigma es que nadie sabe quién eligió a quién), los sistemas de las elecciones online actúan en sentido contrario para asegurarse de que nadie pueda saber la forma en que las personas votaron.

Cuando los partidarios del VPI señalan que el sistema bancario *online* o el de compras por Internet "operan bien", pierden de vista que los riesgos que son aceptables en el ámbito bancario -donde lo que está en juego es el dinero y en caso de fraudes es devuelto a la persona por su banco- son por completo inaceptables en el ámbito del derecho a votar y la democracia, donde si el voto es manipulado no sólo se viola un derecho fundamental sino que se pone en riesgo la legitimidad de las elecciones. Las consecuencias de seguridad son abismalmente distintas, en particular cuando sabemos que es posible que la manipulación de una elección ni siquiera pueda detectarse. La forma en que funcionan los bancos no es la forma en que funcionan las elecciones, ni sus riesgos son trasladables sólo porque ambos sistemas "funcionan" en Internet.[85]

85. El hecho de que todo sistema conectado a Internet pueda tener fallas y vulnerabilidades no hace que éstas signifiquen lo mismo en todos los ámbitos sociales, jurídicos y políticos. Lo que es cierto y preocupante es que siempre puede haber vulnerabilidades que ni siquiera conocemos porque no se han revelado o porque aún no han sido explotadas, tal como pasó en Estonia, que utilizó por más de una década un sistema de VPI antes siquiera de saber que era inseguro y podía ser fácilmente *hackeado*. Al respecto ver: Newman, Lily Hay. *Online Voting Has Worked So Far. That Doesn't Mean It's Safe,* WIRED, May 12 2020. Disponible en: https://www.wired.com/story/online-voting-worked-so-far-doesnt-mean-safe/.

Sabemos que las evaluaciones que los gobiernos realizan para probar sus sistemas de VPI suelen ser parciales e incompletas (porque limitan el análisis del sistema, el tiempo del mismo o por la secrecía de sus resultados). También sabemos que cuando existe tiempo suficiente para que las expertas y expertos independientes hagan ingeniería inversa y una revisión profunda, **siempre se encuentran vulnerabilidades y riesgos** (que normalmente son minimizadas por los gobiernos o las empresas que impulsan el voto por Internet).[86]

Comprender la naturaleza de las votaciones por Internet y el dilema integridad-secrecía nos deja en un callejón sin salida en el que todo parece apuntar a que, en última instancia, uno debe elegir qué sacrificar para obtener el resultado que desea: si optamos por el VPI y sus mecanismos de secrecía, sacrificamos la posibilidad de defender la integridad del voto porque cualquier manipulación se vuelve invisible; si optamos por mecanismos que fortalezcan la integridad (como un recibo en papel con la intención del voto), ponemos en serio riesgo la secrecía del voto.[87]

La pregunta final ante este panorama es por qué deberíamos conformarnos a llevar a cabo esta elección, sobre todo cuando otros medios de votación parecen ofrecer mejores alternativas. ¿Por qué contentarnos con la promesa del optimismo tecnológico cuando lo que nos exige a cambio es que la legitimidad de las elecciones se vuelva un acto de fe?

86. A esta altura ya entendemos la cantidad enorme de riesgos de seguridad existentes tanto en el ámbito de los usuarios como el de los servidores del sistema (y las acciones relacionadas con su puesta en marcha), tales como la activación del sistema, el uso de dispositivos para ello, las llaves criptográficas, etc. (sin mencionar los riesgos "internos" de corrupción de las autoridades, que nunca deben descartarse). Ante todo lo que puede salir mal, desafortunadamente sabemos que las autoridades normalmente actúan sin los cuidados ni los conocimientos suficientes para mitigar los riesgos, y que la complejidad del sistema de VPI lleva casi siempre a descuidos en su uso y a maximizar las posibilidades de comprometer una elección. El análisis que realizamos sobre México a continuación es también (como lo fueron el de Estonia y EUA) muestra de ello.

87. Podemos decir que el voto por Internet tiene un doble problema de invisibilidad. Primero, porque su estudio y revisión normalmente se hace de manera parcial y controlada, 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 mismo 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 sea invisible.

PARTE III / El modelo sobre el Voto por Internet y el caso mexicano en la Ciudad de México

Después del recorrido hecho por la dimensión técnica y por las experiencias comparadas de los casos paradigmáticos que analizamos para entender el funcionamiento, las particularidades y los principios normativos relacionados con el VPI, llegó el momento de desarrollar el modelo que se adecua tanto al derecho fundamental a votar como a los principios democráticos de las elecciones.

Nuestra propuesta sirve para sistematizar y ordenar los requisitos mínimos que todo sistema de voto por Internet debería cumplir para ser satisfactorio, para no poner en riesgo las elecciones ni limitar el derecho a votar de manera libre y secreta, y para no mermar la legitimidad de las elecciones en las democracias modernas. A partir del modelo, podemos evaluar críticamente el sistema de VPI más desarrollado e impulsado en México hasta la fecha, así como las posibles propuestas que surjan más adelante sobre el tema.

1. El modelo democrático del voto frente a su uso en Internet

El modelo democrático resulta de unir dos ejes que corren paralelos en el ámbito de las democracias modernas: por un lado, el eje normativo del derecho al voto y, por otro lado, el eje que de los principios rectores de las elecciones. El resultado de ello es un marco completo que incluye los requisitos jurídicos y técnicos mínimos que deben ser respetados sin excepción para sostener que una elección 1) respeta el derecho de todas las personas a votar de manera libre y secreta y 2) lo hace dentro del marco de elecciones auténticamente democráticas.

El derecho al voto universal, libre y secreto es uno de los pilares normativos de las democracias modernas y es, en este sentido, uno de los triunfos más importantes del desarrollo de las sociedades contemporáneas porque implica la participación de las personas en su comunidad y el

reconocimiento de los principios de la representación y la voluntad popular. La Declaración Universal de Derechos Humanos (DUDH), por ejemplo, reconoce estos elementos en su artículo 21 y señala que esa voluntad debe expresarse por medio de elecciones auténticas y periódicas que incorporen estos principios.[88] El Pacto Internacional de Derechos Civiles y Políticos, por su parte, incorpora estas reglas en su artículo 25, en particular en el inciso b), donde subraya tanto la necesidad de contar con elecciones auténticas como con los principios del voto (universal, igual y secreto).[89]

La Convención Americana sobre Derechos Humanos (CADH)[90] prácticamente replica este artículo para reconocer el valor de los derechos políticos de todas las personas (artículo 23). También especifica que ni siquiera en el caso de peligro público u otra emergencia que amenace la seguridad de cualquier Estado parte pueden ser suspendidos (artículo 27) debido a la importancia que tienen para el fortalecimiento de la democracia y para otros derechos como la libertad de expresión, la de reunión y la de asociación. Por esta razón, la Corte Interamericana de Derechos Humanos (CoIDH) reconoció que el ejercicio efectivo de estos derechos constituye un fin en sí mismo y, a la vez, un medio fundamental para que las democracias modernas garanticen los derechos humanos a todas las personas.[91]

Todos los Estados parte de la CADH tienen la obligación de "generar las condiciones y los mecanismos óptimos para que los derechos políticos puedan ser ejercidos de forma efectiva, respetando el principio de igualdad y no discriminación". Además, el derecho al voto es un derecho esencial que implica que los ciudadanos puedan decidir "directamente y elegir libremente y en condiciones de igualdad" a sus representantes en este sentido,

88. Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948, Resolución 217 A(III), Asamblea General de las Naciones Unidas. Disponible en: https://www.un.org/es/universal-declaration-human-rights/#:~:text=La%20Declaraci%C3%B3n%20Universal%20de%20los,historia%20de%20los%20derechos%20humanos.&text=La%20Declaraci%C3%B3n%20establece%2C%20por%20primera,a%20m%C3%A1s%20de%20500%20idiomas.

89. Pacto Internacional de Derechos Civiles y Políticos, 23 de marzo de 1976 (entrada en vigor), Resolución 2200 A (XXI), Asamblea General de las Naciones Unidas. Disponible en: https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx.

90. Convención Americana sobre Derechos Humanos, 7 al 22 de noviembre de 1969, Organización de Estados Americanos. Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.

91. CIDH. Caso Castañeda Gutman vs México. Sentencia de 6 de agosto de 2008. Excepciones preliminares, Fondo, Reparaciones y Costas. Serie C, No. 184, párrafos 140-141 y 143. En el mismo sentido: CIDH. Caso López-Mendoza vs. Venezuela. Sentencia de 1 de septiembre de 2011. Fondo, Reparaciones y Costas. Serie C, No. 232, párrafo 108.

siempre en línea de los principios rectores del mismo. Aunque ni la CADH ni la CoIDH establecen un marco rígido ni un único sistema electoral para volver estos principios efectivos, sí es claro que su reglamentación debe cumplir "con los requisitos de legalidad, esté dirigida a cumplir con una finalidad legítima, sea necesaria y proporcional".[92]

Al mismo tiempo, la obligación de los Estados en materia político-electoral debe seguir estas "directrices específicas" para garantizar la autenticidad de las elecciones. Existe un "mandato específico" hacia los Estados de que dichas elecciones garanticen en todo caso la libertad, la secrecía y la universalidad del voto en la modalidad que elijan, para cumplir así su obligación general de garantizar los derechos, lo que significa que deben adoptar medidas concretas tanto organizativas como institucionales para asegurarse de que esto sea así. La CoIDH ha señalado que, además de las obligaciones relacionadas al goce de este derecho, existe desde la CADH (en su artículo 23.1) la obligación de asegurarse que las ciudadanas y ciudadanos cuenten con "la oportunidad real" de ejercerlos plenamente, y que esto implica encargarse de elegir medidas que vayan en esta dirección.[93]

Por otro lado, la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en su artículo 1o reconoce el máximo rango normativo a los tratados internacionales de derechos humanos y establece la obligación de garantizar los mismos (entre otras). También reconoce el derecho a votar en elecciones libres, auténticas y periódicas a partir del sufragio universal, libre, secreto y directo (de acuerdo a sus artículos 35, Fr. I y 41, Fr. I, párr. 2), y los principios orientadores de la función electoral y la organización de las elecciones para las autoridades electorales: certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad (artículo 41, Fr. V, Apartado A, primer párrafo).

Esto es lo que el Tribunal Electoral del Poder Judicial de la Federación (TEPJF) ha reconocido como los "principios rectores de la función electoral

92. CIDH. Caso Castañeda Gutman vs México. Sentencia de 6 de agosto de 2008. Excepciones preliminares, Fondo, Reparaciones y Costas. Serie C, No. 184, párrafos 145, 147 y 149, respectivamente a cada cita. Toda medida que pueda constituirse en una restricción al derecho a votar debe ser proporcional y razonable en el sentido de no ir más allá de las causales habilitantes de los derechos políticos, como pueden ser la edad mínima para votar y ser votado. Al respecto ver: CIDH. Caso Argüelles y otros vs. Argentina. Sentencia de 20 de noviembre de 2014. Excepciones preliminares, Fondo, Reparaciones y Costas. Serie C, No. 288, párrafo 222.

93. Caso Yatama Vs. Nicaragua. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 23 de junio de 2005. Serie C No. 127, párrs. 195 a 200.

y las características del voto": máxima publicidad, transparencia, rendición de cuentas y certeza. A su vez, los principios rectores se articulan con los principios constitucionales del derecho al voto universal, libre, secreto y directo.[94]

Cuando pensamos el marco constitucional, regional e internacional en la materia, y lo insertamos en las dimensiones técnicas y comparadas de otras experiencias para situar la discusión sobre el VPI, es posible sistematizar los principios base del modelo y darles contenido pensando específicamente en los sistemas de voto por Internet. Esquemáticamente, el modelo consiste en lo siguiente:

Todo sistema de voto por Internet debe:

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*).

→ Este elemento implica que el sistema de VPI debe garantizar que: ninguna falla de seguridad pueda afectar alguno de estos requisitos, que los votos no puedan ser manipulados y, por consiguiente, que el sistema no pueda ser manipulado para cambiar una elección.

ii) La secrecía consiste en que ninguna persona pueda conocer la intención del voto de las y los electores aún cuando ellos quieran mostrarlo.

→ Este elemento implica que el sistema de VPI cuente con los mecanismos que aseguren la imposibilidad de asociar la intención del voto de una persona con el voto emitido dentro del sistema.

94. TEPJF. MECANISMOS DE DEMOCRACIA DIRECTA. EN SU DISEÑO DEBEN OBSERVARSE LOS PRINCIPIOS CONSTITUCIONALES PARA EL EJERCICIO DEL DERECHO HUMANO DE VOTAR. Tesis XLIX/2016. Gaceta de Jurisprudencia y Tesis en materia electoral, Tribunal Electoral del Poder Judicial de la Federación, Año 9, Número 18, 2016, páginas 96 y 97.

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 (familia, trabajo, partidos políticos, representantes, etc.).

→ Este elemento implica que el sistema debe garantizar que el voto de las personas esté libre de coerción para mantener su carácter efectivamente libre.

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.

→ Este elemento implica la exigencia de pruebas de penetración recompensa, de la permisión de realizar ingeniería inversa para encontrar vulnerabilidades de seguridad en los sistemas de VPI, de la revisión completa de los códigos fuente, *hardware* y *software* con los que funciona el sistema y, finalmente, de la publicación completa de la información que resulte de estos estudios, que deberá estar al alcance

de toda la ciudadanía y deberá ser comprensible para ella, también, sin conocimientos técnicos especializados.

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.

→ Este elemento implica que las tecnologías de la información y la comunicación no están exentas de su adecuación dentro del marco de respeto de los límites que las restricciones a los derechos humanos deben cumplir. El hecho de que los derechos se encuentren en el entorno digital de Internet no significa, en este sentido, que las reglas con las que funcionen desaparezcan o estén exentas de su cumplimiento.

A partir de esta base podemos evaluar el sistema desarrollado en los últimos años en la Ciudad de México, al tiempo de evaluar el cumplimiento del mismo frente a los supuestos beneficios del voto por Internet.

1. Antecedentes y marco normativo del VPI en México

El voto por Internet no es nuevo, al menos a nivel local. El Instituto Electoral de la Ciudad de México (IECM), antes del Distrito Federal (IEDF), es la autoridad electoral referente que desarrolló un sistema desde el 2010 para las y los rsidentes en el extranjero (aunque otros Estados también lo implementaron de distintas formas) en algunas modalidades de votación (para la Jefatura de Gobierno y para los mecanismos de participación ciudadana). A nivel nacional, tanto la pandemia por el COVID-19 como el impulso en los últimos años por el Instituto Nacional Electoral (INE) han hecho que su aprobación se vuelva prácticamente inminente.[95] La revisión del modelo del

95. Excelsior. *Coronavirus impulsa el voto vía remota; INE probará sufragio por Internet en el 2021,* Aurora Zepeda, 22 de mayo de 2020. Disponible en: https://www.excelsior.com.mx/nacional/coronavirus-impulsa-el-voto-remota-ine-probara-sufragio-por-internet-en-2021/1383535. La intención es clara tanto por la aprobación de lineamientos generales que sirven como primeros pasos hacia el establecimiento del sistema como por el inicio de la convocatoria para realizar una auditoría a nivel nacional del sistema de VPI y su adjudicación por concurso a la empresa *Deloitte & Co. S. A.* y *Deloitte Asesoría en Riesgos, S. C.* a través de la licitación hecha por Galaz, Yamazaki, Ruiz Urquiza, por el monto de 22,851,750.00 (veintidós millones ochocientos cincuenta y un mil setecientos cincuenta pesos mexicanos). Al respecto ver la resolución LP-INE-003-2020 que puede encontrarse aquí: https://www.ine.mx/licitaciones/.

IECM es útil para pensar las posibles consecuencias o implicaciones de desarrollar el voto por Internet a nivel nacional.[96]

El derecho de las y los mexicanos a votar en el extranjero existe desde el año 2006 en la CPEUM. En el proceso electoral federal de la Presidencia del 2006 y el de 2012, la modalidad de voto en el extranjero se realizó únicamente por la vía postal, mientras que en el 2012 se realizó por vías postal y electrónica para la entonces Jefatura de Gobierno del DF (y en el año 2018 únicamente se realizó por vía postal). El llamado Sistema Electrónico por Internet (SEI) del IECM ha sido usado por varios años también para las Consultas Ciudadanas sobre Presupuesto Participativo, en numerosas ocasiones.[97]

El 20 de diciembre de 2010 el Poder Legislativo del DF incorporó la posibilidad de que las personas votaran desde sus lugares de residencia cuando se tratare de ciudadanas y ciudadanos residentes en el extranjero (en el entonces Código de Instituciones y Procedimientos Electorales del Distrito Federal, CIPEDF). Poco después, el IEDF emitió un Acuerdo que estableció los mecanismos para recabar el voto de los ciudadanos del DF en el extranjero para elegir el cargo de Jefe de Gobierno (2011-12).[98]

El SEI fue registrado el 19 de diciembre del 2013 bajo derechos de autor por el IEDF. A partir de allí, la normatividad electoral cambió varias veces tanto a nivel constitucional (en materia electoral) como local. En el 2016 se expidió el Reglamento de Elecciones del INE (anteriormente Instituto Federal Electoral -IFE-) (base legal que regula los distintos temas relacionados con el proceso electoral y el voto) y posteriormente se aprobaron los "Lineamientos para el Desarrollo del Sistema del voto electrónico por internet para mexicanos residentes en el extranjero", a través del Consejo General del INE (INE/CG770/2016).

96. Además de la Ciudad de México al menos otros diez estados que tienen regulado el voto en el extranjero exploran, junto con el INE, el uso de un SEI para las elecciones locales del 2020-21. Baja California Sur, Chihuahua, Colima, Guerrero, Michoacán, Nayarit, Querétaro, San Luis Potosí y Zacatecas, así como para una diputación migrante y una de representación proporcional de los estados de Guerrero y Jalisco, respectivamente. Noticias Electorales. "(México) Concluye INE Simulacro de voto electrónico por Internet con éxito", 30 de marzo de 2020. Disponible en: https://www.noticiaselectorales.com/mexico-concluye-ine-simulacro-de-voto-electronico-por-internet-con-exito/.
97. Desarrollamos las estadísticas de todas estas elecciones y participaciones más arriba en la Parte I del trabajo al referirnos a los argumentos sobre la participación política y a los costos del VPI.
98. El Consejo General del entonces IEDF, hoy IECM, a través del Acuerdo ACU-69-11.

Entre su implementación en el año 2012 y la actualidad, existió un cambio legal que derivó en la nueva Constitución de la Ciudad de México (el 5 de febrero de 2017) y en la abrogación del CIPEDF, para establecer el nuevo Código de Instituciones y Procedimientos Electorales de la Ciudad de México (CIPECM) (el 7 de junio de 2017).[99] Además, la Constitución Política de la Ciudad de México en su artículo 7, apartado F ("Derecho a un Gobierno democrático y a la participación política paritaria"), numeral 3, establece que las personas originarias de la Ciudad que residen fuera del país, tienen derecho a votar y ser votadas en elecciones locales, de conformidad con lo previsto en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), esa Constitución y las leyes aplicables.

Junto con esas disposiciones, la Ley General de Instituciones y Procedimientos Electorales del 23 de mayo de 2014 (LGIPE) habilita el voto de las y los mexicanos en el extranjero con la posibilidad de realizar el "ejercicio del voto electrónico", facultando al Consejo General del instituto electoral correspondiente para aprobar los formatos y modalidades, así como el uso de herramientas y materiales (artículo 339), sea para la elección la Presidencia de la Nación, las Gubernaturas o la Jefatura de Gobierno del Distrito Federal (ahora CDMX) (artículo 329, párrafos 1 y 2), a condición de que los lineamientos que se emitan para que se realice **"deberán asegurar total certidumbre y seguridad comprobada a los mexicanos residentes en el extranjero, para el efectivo ejercicio de su derecho de votar en las elecciones populares"** (artículo 329, párrafo 3).[100]

El CIPECM reconoce explícitamente que la máxima publicidad, la transparencia, la rendición de cuentas y la certeza son principios rectores de la función electoral y que se articulan con los principios elementales del sufragio (universal, libre, secreto y directo).[101] A partir de ellos, el IECM desarrolló el SEI desde el marco dado por el reconocimiento de los mecanismos de democracia directa como vías para el ejercicio del voto (artículo 35,

99. Para ver las distintas modificaciones, mesas de trabajo, acuerdos relacionados y decisiones administrativas en el medio ver: IECM. (Acuerdo IECM/ACU-CG-014/2017), pp. 2-4.
100. Como quedará claro a lo largo de este apartado, también la legislación que regula las elecciones tanto a nivel nacional como para la Ciudad de México da soporte al modelo que proponemos para evaluar los sistemas de voto por Internet.
101. TEPJF. MECANISMOS DE DEMOCRACIA DIRECTA. EN SU DISEÑO DEBEN OBSERVARSE LOS PRINCIPIOS CONSTITUCIONALES PARA EL EJERCICIO DEL DERECHO HUMANO DE VOTAR. Tesis XLIX/2016. Gaceta de Jurisprudencia y Tesis en materia electoral, Tribunal Electoral del Poder Judicial de la Federación, Año 9, Número 18, 2016, páginas 96 y 97.

Fr. VII y VIII de la CPEUM) y de los lineamientos del INE resultantes de la permisión del artículo 329 de la LGIPE.[102] Tal como desarrollamos en la Parte I, además del uso del SEI en el proceso electoral del 2012, se utilizó en las Consultas Ciudadanas sobre Presupuesto Participativo en numerosas ocasiones.

2. Particularidades del Sistema Electrónico por Internet del IECM en la CDMX

El sistema actual de VPI fue construido por IECM mismo, quien lo considera un referente en seguridad y sistemáticamente destaca su fortaleza en seguridad al asociarlo con el uso de los bancos en Internet.[103] También sostiene que -siguiendo las guías del *Grupo de Trabajo de Especialistas* (conformado en el 2013 por el INE) y los Lineamientos del INE- el sistema ha demostrado "alcanzar la madurez de su Plataforma Tecnológica Operativa con la que se resuelva y dé cumplimiento a dichos retos con **certeza absoluta y seguridad garantizada;** y hacer un análisis exhaustivo del grado de cumplimiento normativo".[104]

La forma en que el sistema se relaciona con los principios centrales del derecho al voto, de acuerdo a las propias declaraciones del Instituto es la siguiente:

- Universal: La universalidad del sufragio se garantiza para todas las y los ciudadanos que cumplan con los requisitos legales para ejercer su derecho al voto.
- Libre: **Se ejerce con absoluta libertad y responsabilidad**, en este caso, desde el lugar que la o el ciudadano haya destinado para ejercer su derecho y siempre que se haya registrado en el Listado Nominal correspondiente, únicamente necesita un medio electrónico o computadora conectada a internet desde el extranjero.
- Secreta: La secrecía se manifiesta en dos principales etapas, la primera con el hecho de solicitar la contraseña que es única y que se asigna de manera aleatoria,

102. Ver el Acuerdo INE/CG196/2017, en su considerando QUINTO.
103. "En adición a lo anterior, se tiene plena coincidencia sobre la opinión de que actualmente se realizan miles de transacciones electrónicas todos los días en todo el mundo, muchas de estas de índole bancario, resultando estas funcionales seguras, confiables y efectivas, utilizando muchos de los candados o sistemas de seguridad antes mencionados". Ver: IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación*, julio de 2017. Disponible en: https://www.iecm.mx/www/taip/cg/acu/2017/IECM-ACU-CG-014-2017.pdf.
104. IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación*, julio de 2017, p. 5.

sin conocimiento de ningún funcionario público sino a través de un sistema con el cifrado que no permite identificar a la o el ciudadano con ésta y en segundo término, cuando el ciudadano realiza la votación; el voto se transporta por la red a través de un algoritmo cifrado con altos niveles de seguridad que no permite identificar los datos personales de la o el ciudadano con su elección y tampoco el sentido del voto.[105]

- Directa: Únicamente el propio ciudadano puede entrar al sistema y solicitar su contraseña.

[Los énfasis son nuestros]

El discurso del IECM se ha mantenido con el tiempo. En la reunión realizada para la presentación del SEI frente a organizaciones de la sociedad civil el 20 de enero de 2020, los argumentos sobre la seguridad y los riesgos del sistema fueron los mismos. Supuestamente, el SEI respeta con "certeza absoluta" los principios del voto, apoyado en la criptografía, la aleatorización y los elementos de seguridad que dan las tecnologías actuales. Además, el Instituto justifica, una y otra vez, el uso legítimo del VPI porque sus características y particularidades "fueron confirmadas" por una multicitada sentencia de la Sala Superior del TEPJF.

Esta afirmación es problemática. La sentencia (que analizamos en seguida) revisó y legitimó la versión del SEI existente en el 2012 que luego cambió sustantivamente durante los años. También sabemos que la particularidad del voto por Internet obliga a su evaluación constante, por lo que una sentencia o aprobación administrativa de hace casi diez años es irrelevante en términos sustantivos para legitimar un sistema posterior de VPI (la legitimidad del pasado no puede dar legitimidad en el presente).[106] Además, queda el detalle de que las sentencias judiciales no son infalibles. No es raro que en temas donde la tecnología y el conocimiento técnico son centrales para determinar las consecuencias jurídicas, una decisión judicial pueda estar equivocada, tal como sucede con la sentencia del TEPJF. [107]

105. En la Parte I del trabajo mostramos lo relativamente fácil que es poner en riesgo el voto y una elección frente a las protecciones de cifrado. La existencia de *malware* y los riesgos "correspondientes al usuario" hacen que un atacante pueda tomar control del dispositivo y cambiar el voto, así como poner en juego la secrecía del mismo a pesar de los procesos de encriptación.

106. La sentencia referida reconoce como principio general la facultad que tienen los Institutos Electorales, de acuerdo a la normatividad vigente, de implementar mecanismos para garantizar el voto, abriendo la posibilidad a formatos electrónicos (aunque no los mencione expresamente). En términos jurídicos esta disposición puede permanecer en el tiempo si las bases normativas no cambian. Pero es muy distinto la parte concreta sobre el sistema analizado en ese momento por el Tribunal, cuya validación alcanzaba ese sistema en ese momento concreto.

107. Lo que queremos decir es que, primero, el argumento del IECM es inconsistente porque no justifica lo que dice justificar y, segundo, que aún desde su argumento, la sentencia en la que se apoya está plagada de errores y problemas jurídicos, interpretativos y técnicos.

El SEI inició una segunda etapa de desarrollo cuando se amplió su uso para la recepción de opiniones en las "Consultas Ciudadanas sobre Presupuesto Participativo", a partir del 2012 y fue revisado y modificado en distintas ocasiones: en en el 2012 (revisado por el Instituto Politécnico Nacional y con un sistema adquirido a un tercero); en el 2013-2014 con el sistema desarrollado conjuntamente con la UNAM (con revisión del ITESM y la UNAM para el desarrollo del sistema propio del IECM y su infraestructura); en el 2015 con análisis y "puesta a punto de infraestructura" con la empresa DRONET; en el 2016 con una revisión de sistema "por parte de Comité Técnico Asesor (COTESEI) y la Organización de Estados Americanos y una "empresa externa"; y en el 2017 nuevamente con COTESEI para la revisión del sistema, al tiempo de trabajar la "implementación de mejoras de seguridad" con la empresa SCANDA.[108] Finalmente el sistema fue revisado nuevamente en el 2020 por la UNAM (FES Aragón) y por otra empresa privada.

El IECM nos dice que su sistema ha ido mejorando con el tiempo, que cuenta con una infraestructura "de alta disponibilidad y diversos procedimientos operativos", con mecanismos de seguridad, de monitoreo y "auditorías informáticas robustas" (la adecuación y modernización del sistema reúne al menos tres sectores: empresas especializadas en tecnología, universidades e institutos especializados en la materia y las instituciones electorales). Dentro de las características principales relacionadas con la seguridad e integridad del voto están:

- La carga de la lista nominal y cómputo de la elección se realiza en minutos, gracias a la optimización y correcta configuración de las bases de datos.
- La disociación del voto se realiza al momento de almacenar el voto, por lo que no se requiere de un proceso especial previo al cómputo.
- Cuenta con los mecanismos de seguridad que garantizan el resguardo y secrecía de los votos.
- Cuenta con un módulo de pre registro y seguimiento de los ciudadanos que desean emitir su voto a través de esta modalidad.
- Ostenta un mecanismo de doble factor de autentificación a través de la entrega de contraseña de manera presencial y por mensaje SMS.

108. IECM. Voto desde el extranjero bajo la modalidad electrónica. *Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación*, julio de 2017, pp. 9-11.

- Utiliza la autoridad certificadora propia del Instituto, que garantiza que todos los votos serán firmados electrónicamente por su propia arquitectura, legitimando cada voto emitido.

- Utiliza una llave privada en cada servidor, para certificar que los votos almacenados, fueron generados a través de la infraestructura del Instituto, imposibilitando la generación de votos apócrifos.

- La plataforma tecnológica que ha sido utilizada está diseñada con una arquitectura de alta tecnología y de alta disponibilidad, misma que es sometida a procesos de mantenimiento y puesta a punto, previos a la operación de cada ejercicio.

- Todos los movimientos son almacenados en una bitácora, que puede ser auditada en todo momento.

- Cuenta con diversos módulos de monitoreo en línea que permiten dar seguimiento puntual al proceso de votación.[109]

En la actualidad, el sistema tiene una etapa de pre-registro en la que se cargan distintos datos personales de las y los votantes antes de la jornada electoral. Los datos personales quedan almacenados hasta por dos meses. Posteriormente se hace una votación remota desde el dispositivo móvil o la computadora de la persona, o de manera presencial en algún centro de votación autorizado en la CDMX (utilizando boletas electrónicas y sin dejar ningún registro impreso de papel); luego se lleva a cabo la jornada electoral y se contabilizan tanto los votos en papel como los votos electrónicos.

El sistema pide al votante un correo electrónico que queda vinculado a la identidad de la persona, un número de teléfono celular que también se vincula y la información de la Credencial para Votar con Fotografía (CVCF) (donde están almacenados otros datos personales). La App de votación utiliza luego un sistema de validación con reconocimiento facial con el que se pide a la persona que verifique su identidad. La versión que se usó en el año 2018 funcionaba de la siguiente manera:

a) En los días previos al inicio de operaciones del Sistema de voto, las y los ciudadanos recibirán un correo electrónico, en el que se les indicará que el Sistema se encontrará disponible para realizar la emisión de su voto en el periodo del 23 de junio al 1 de julio de 2018.

b) Una vez que la o el ciudadano ingresa al Sistema, se le solicita un medio de autenticación, que consiste en la clave de elector y la contraseña recibida.

c) La o el usuario ingresa su clave de elector y la contraseña de voto electrónico.

109. *Ibidem*, pp. 12-13.

d) El Sistema valida la información ingresada, si los datos son correctos, se desplegará la "Boleta Virtual" con las opciones de votación.

e) A través de la "Boleta Virtual", la o el ciudadano puede elegir la opción de su preferencia para elegir al Jefe o Jefa de Gobierno, y pulsará el botón de votar.

f) El Sistema presentará una pantalla de confirmación, mediante la cual la o el ciudadano tendrá la opción de confirmar o corregir su voto; al confirmarlo, éste se enviará y depositará en la urna virtual. Es importante señalar que el sistema únicamente permitirá la elección de una opción, por lo que solo cuando el ciudadano confirme su voto, éste se depositará en la "Urna Virtual".

g) Al confirmar su sentido del voto, el Sistema cifrará la información correspondiente al voto con la llave electrónica de la elección, y la firmará electrónicamente para asegurar su integridad, autenticidad y privacidad.

h) El Sistema almacenará la información correspondiente al voto en una urna virtual, alojada en los servidores centrales del Instituto.

i) Al finalizar la votación del ciudadano, el Sistema presentará una pantalla que contiene el recibo de voto, confirmando la recepción del mismo. Este recibo de voto permitirá a la o el elector verificar que su boleta fue registrada de manera correcta en la urna virtual. Este recibo no contiene ninguna información sobre las opciones seleccionadas por la o el elector, de manera que garantiza la privacidad de voto y únicamente otorga a la o el elector la seguridad de que su voto será tomado en cuenta.

Finalmente, los recibos de voto se publicarán en la página de Internet del IECM www.iecm.org.mx para que los electores puedan comprobar que su recibo está en la lista y, por tanto, su voto fue contado.[110]

Una vez que los votos son emitidos desde el teléfono (aunque también puede hacerse en los "Módulos de votación presencial"), por ejemplo, el sistema realiza un proceso de aleatorización de los mismos para separar la identidad de las votantes con el sentido de sus votos, que son luego enviados a una urna electrónica (el proceso que en apartados anteriores describimos como "mixnet"). Todo recuento únicamente puede hacerse desde el sistema mismo, ya que no existe ningún registro en papel que respalde los votos de las personas. Los datos son encriptados, se usa una firma electrónica y se resguarda la secrecía del voto por medio del sistema de aleatorización.

Por otro lado, **el código de la aplicación es cerrado** y se da únicamente a los sujetos que realizan las auditorías (muchas veces incompleto), las cuales son pagadas por el propio IECM. Los informes de los intentos de

110. IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Operativa Procedimental*, julio de 2017, pp. 5-6.

hackeo o incidentes de seguridad -que el propio IECM reconoce que existen- no son públicos ni existen como informes internos tampoco. En este sentido, toda evaluación y revisión del código, el sistema en general y las particularidades del mismo no están abiertas a pruebas de penetración y recompensa, ingeniería inversa ni a evaluaciones independientes fuera del control y gestión del IECM.[111]

El sistema usa servidores internos que realizan distintas funciones. En la votación, deben cargarse los archivos de las llaves privada y pública con las que ésta se realiza. La configuración y apertura del sistema se hace en una sesión del Consejo General, donde se registra que la urna virtual (el sistema usa varias urnas virtuales) no tenga registros o votos emitidos (que esté en ceros).[112]

El IECM cuenta con un catálogo de riesgos de seguridad que reconoce dentro del funcionamiento del sistema y que usa para los análisis de riesgo con los que pone a prueba el SEI. En este punto en particular, señala que una medida de mitigación importante para el buen funcionamiento es que cuenta con equipos *(hardware)* extra que pueden usar para sustituir los que usan en la elección si estos fallan. También que tiene pólizas de soporte técnico con los fabricantes del *hardware* con el que el SEI funciona (e igual con los equipos de seguridad y sus acciones de mitigación) en caso de que lo necesiten. Todos estos puntos se consideran como riesgos "controlables" por el Instituto.[113]

Aquí es muy importante señalar algo sobre lo que hacíamos énfasis en el apartado sobre los riesgos del VPI en la Parte I del trabajo: la existencia de distintos componentes de *hardware* y *software* internos y externos son vulnerabilidades potenciales e implican riesgos para una elección (por su facilidad de infectarlos). Si algo falla en una elección y una pieza debe cambiarse o debe realizarse un ajuste al *software* en ese momento, se abre una ventana de riesgo de manipulación de la elección. Al mismo tiempo, si el

111. El reconocimiento de intentos de hackeo al sistema en los últimos años se hizo públicamente en la reunión del IECM con representantes de la sociedad civil que tuvo lugar en las instalaciones del instituto, el 20 de enero del 2020, donde R3D participó e hizo preguntas relacionadas con este punto.
112. Los "componentes de la infraestructura" del SEI se integran por: el equipo de comunicaciones del Instituto, los "enlaces de Internet" con diferentes ISP para la comunicación entre el SEI e Internet, los servidores donde se registra la información de los votos, el centro de cómputo físico donde está la infraestructura del Voto Electrónico en el Instituto y los suministros de energía eléctrica del Centro de Cómputo del IECM. IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación*, julio de 2017, pp.
113. *Ibidem*, pp. 21-24. El IECM sólo considera seis grupos de riesgos: Sistema, Equipos de comunicaciones, Equipos de seguridad, Enlace de Internet, Bases de datos y Energía eléctrica.

programa se echa a andar con dispositivos que no son auditados previamente y cuyo único propósito es el de utilizarse en la elección, nuevos riesgos de comprometer el sistema se presentan. El problema es que parece que el IECM no contempla estas posibilidades siquiera dentro de sus análisis de riesgo y que, peor aún, estas eventualidades efectivamente sucedieron las últimas veces que el sistema se utilizó (explicamos este punto en detalle más adelante).

3. Análisis jurídico de las sentencias. decisiones técnicas y auditorías especializadas

El IECM basa prácticamente toda la justificación normativa del SEI en la sentencia del TEPJF que en el año 2012 consideró que el sistema de VPI implementado por el Instituto Electoral en ese entonces garantizaba la seguridad y la integridad del voto de las y los ciudadanos. De manera algo extraña, también, sostiene que la sentencia implica el uso del principio de progresividad de los derechos humanos con respecto al VPI para los ciudadanos residentes en el extranjero.[114] Finalmente, el Instituto señala que las "condiciones jurídicas" habilitantes del VPI resultan no sólo de la normatividad aplicable sino también del trabajo jurisprudencial, de la opinión del Comité Técnico "formado por especialistas en las materias informática, procesos electorales y estrategia política" y también de la "ejecución de auditorías de empresas de prestigio internacional".

> Además de las ventajas con que cuenta el Sistema de Votación Electrónico por Internet, como la erradicación del margen de error humano; la reducción de costos; la emisión del voto desde cualquier lugar, sólo por mencionar algunas ventajas; es una oportunidad para demostrar cualquier duda o desconfianza de este sistema, ya que como ya se especificó en párrafos anteriores, está dotado de certeza y seguridad para la emisión del voto.[115]

El voto por Internet, dice el Instituto, beneficia a las y los ciudadanos en cuatro puntos: por la **simplicidad** para votar y porque no requiere hacer envíos postales complejos ni trámites adicionales; por la **privacidad y comodidad** de "emitir su voto desde el lugar que se elija; evitando así que factores meteorológicos, laborales, políticos y sociales impidan la participación"; por la **disponibilidad** de tener "un amplio plazo de tiempo para realizar el canje

114. IECM. Acuerdo IECM/ACU-CG-014/2017, párrafo 40.
115. Como se observa, el Instituto sostiene los argumentos clásicos de los supuestos beneficios del VPI, que discutimos en la Parte I del trabajo. IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Jurídica Normativa*, julio de 2017, p. 20.

de clave y posteriormente emisión del voto, estando el portal habilitado 24 horas del día sin restricciones"; y por la **certeza** del "conocimiento inmediato de que su voto ha sido emitido y resguardado correctamente mediante un acuse de recibo electrónico".[116] Mientras que los beneficios para el IECM serían (el énfasis es nuestro):

> Seguridad: el sistema posee un alto grado de fiabilidad debido a los procesos de encriptación, **lo cual garantiza que se cumplan los que el voto sea universal, libre, secreto y directo.**
>
> Eficacia: Los procesos automatizados permiten la recepción y resguardo inmediato del voto mexicano en el extranjero **con un grado de certeza máximo a diferencia del voto postal, el cual depende de tiempos, factores y agentes externos.**
>
> Inclusión: Las nuevas herramientas tecnológicas están orientadas a **garantizar la plena inclusión y el ejercicio de los derechos político electorales de los ciudadanos,** así como mecanismos de construcción de ciudadanía. Es decir, **promover la participación política en igualdad de oportunidades entre hombres y mujeres de diversas condiciones.**
>
> Economía: la sistematización en los procesos permite economizar recursos materiales y humanos.[117]

A continuación analizamos de manera detallada la sentencia que sirve como pilar normativo para la defensa del voto por Internet, permitiéndonos por momentos citar en extenso para señalar algunos puntos cuestionables de la misma que suelen pasarse de largo en esta discusión.

a. La Sentencia SUP-JRC-306/2011 de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación

La sentencia del año 2012 es la referencia jurídica principal de justificación para los sistemas actuales de voto por Internet en México (del mismo modo que la analogía con el sistema bancario por Internet es la referencia empírica principal para justificar la supuesta seguridad del VPI).[118] Aunque es importante subrayar, una vez más, que una sentencia que legitimó un sistema electrónico del pasado no sirve para legitimar los del presente, también es importante analizarla para ver si en su substancia se trata de una decisión satisfactoria en materia de derechos humanos y del análisis técnico indispensable para evaluar los sistemas de voto por Internet. Sobre ella, el IECM nos dice lo siguiente:

116. *Ibidem*, julio de 2017, p.1.
117. *Ibidem*, p.2.
118. Todos los énfasis añadidos en las citas textuales de la sentencia son nuestros.

> Asimismo, es importante señalar que la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, al resolver el juicio de revisión constitucional identificado con clave SUP-JRC-306-2011, **señaló que el sistema implementado por este Instituto garantizaba la seguridad del voto de los ciudadanos del otrora Distrito Federal residentes en el extranjero, así como la integridad de la información emitida.**
>
> **Además estimó que el sistema cumplía con los estándares suficientes de seguridad, ya que su funcionamiento es similar al que se utiliza en otros sistemas de Internet para acceder a sitios electrónicos que requieren altos niveles de seguridad y confianza, como es la banca en línea o el procesamiento de compra de diverso productos, en el cual se proporcionan los datos de una cuenta de banco o una tarjeta de Internet, en cuyos casos, las claves de acceso son personales y de responsabilidad de su titular. Lo anterior debe considerarse como un candado, razonable e idóneo para garantizar la emisión del voto de acuerdo con los principios de universalidad, libertad y secrecía, ya que la solicitud, registro y entrega de contraseña, se realiza a través de un procedimiento automático, el cual, debido a sus características técnicas, se realiza de manera objetiva e imparcial.**[119] **[Énfasis añadido]**

Si no quisiéramos ir más lejos, un error fatal para la argumentación jurídica de la sentencia y para la justificación del Instituto es la de creer dos cosas que refutamos en este trabajo: primero, que los sistemas bancarios y los electorales funcionan de la misma manera en Internet (cuando son estructuralmente distintos y sus diferencias vuelven irrazonable su uso indiferenciado); segundo, que las condiciones de seguridad de la banca y las compras en línea son siquiera cercanos a cumplir con los mínimos de seguridad necesarios para proteger el voto y garantizar la legitimidad de una elección en Internet. Esto es particularmente grave porque al momento de la decisión del TEPJF ya existía, no sólo desde la comunidad técnica y la académica sino también desde agencias de gobierno, científicos de la computación y la comunidad *hacker,* muchísima evidencia de que esta asociación no sólo era falsa sino riesgosa en términos de seguridad. El Tribunal ignoró o desconocía la información y utilizó esa idea como un presupuesto de toda su argumentación, cuando debía ser, en dado caso, una conclusión fundamentada.

Pero para ser más claros aún, vamos a detenernos en lo que dice específicamente la sentencia para diseccionarla y mostrar los problemas que no resolvió.

119. IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Jurídica Normativa*, julio de 2017, pp. 12-13.

La Sala Superior resolvió el 12 de enero de 2012 un Juicio de Revisión Constitucional sobre dos fallos emitidos por el Tribunal Electoral del Distrito Federal (TEDF), quien invalidaba dos acuerdos del Consejo General del Instituto Electoral del Distrito Federal (CGIEDF) que establecían la modalidad del VPI para la elección de Jefe de Gobierno del DF (expedientes TEDF-JEL-048/2011 y el TEDF-JEL-049/2011 acumulados).

El Código Electoral del DF del 2010 estableció una modalidad en la que se permitía el "voto electrónico" bajo distintas modalidades que podían ser determinadas por la autoridad administrativa (el CGIEDF). El Consejo emitió el acuerdo ACU-69-11 donde avaló un mecanismo para recabar el voto "electrónico por Internet". El anexo impugnado junto a ese acuerdo se llamó "Procedimiento de votación electrónica por internet", donde se detallaron las características técnicas y jurídicas del mismo. El TEDF revocó el acuerdo y el anexo a partir de los dos juicios acumulados. El proyecto resuelto por la Sala Superior estuvo a cargo del Magistrado Salvador Olimpo Nava, quien revocó las sentencias del TEDF y avaló el acuerdo y su anexo para validar el voto por Internet.

La Sala Superior reconoció que el voto cuenta con cuatro principios fundamentales que le dan su carácter de secreto, libre, universal y directo. Además, en su análisis incorporó dos principios de la "función electoral": la certeza y la objetividad.

> Dichos principios son, entre otros, las elecciones libres, auténticas y periódicas; el sufragio universal, libre, secreto y directo; la certeza, legalidad, independencia, imparcialidad y objetividad como principios rectores del proceso electoral. La observancia de estos principios en un proceso electoral se traducirá en el cumplimiento de los preceptos constitucionales antes mencionados.[120]

Un argumento importante contra las decisiones del TEDF (hecho por el Partido de la Revolución Democrática -PRD-) fue el siguiente:

> "La modalidad de voto electrónico por internet no vulnera las características del sufragio y los principios rectores de la función electoral establecidos en la Constitución federal (legalidad y certeza), porque ello es materia, en su caso, de la nulidad de la votación o de la elección de Jefe de Gobierno del Distrito Federal. Las medidas de seguridad y las etapas que se establecen en el Acuerdo ACU-069-11, su Anexo Técnico y en el Procedimiento de votación electrónica por internet (especialmente en el numeral 3) proporcionan certeza y las herramientas técnicas para el ejercicio del voto en términos de ley, así como también se hace en

120. Apoyándose en la tesis: ELECCIONES. PRINCIPIOS CONSTITUCIONALES Y LEGALES QUE SE DEBEN OBSERVAR PARA QUE CUALQUIER TIPO DE ELECCIÓN SEA CONSIDERADA VÁLIDA. Publicada en *Jurisprudencia y Tesis Relevantes* 1997-2005, tomo tesis relevantes, páginas 525-527.

el Acuerdo ACU-47-2011. El Instituto Electoral del Distrito Federal privilegió el derecho a votar y confió en la responsabilidad y formación cívica del ciudadano."

Uno de los agravios establecidos por el PRD fue que el TEDF había desplazado el principio de la universalidad del voto en favor de los principios de certeza y seguridad jurídica, lo que constituía un error de interpretación constitucional:

> "La responsable realizó una ponderación de derechos de índole constitucional, en detrimento de la universalidad del voto y para favorecer los principios de certeza y seguridad jurídica, lo cual es incorrecta, incompleta y equivocada. Lo anterior, para el actor, es una extralimitación de dicho tribunal local y ejerce una atribución exclusiva de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, a pesar de que con dicho sistema de votación se protegía el derecho de recibir votos a favor del partido político para el candidato a ese cargo de elección popular."

La Sala Superior reconoció que las y los legisladores tenían la facultad de reglamentar el voto, siempre de acuerdo a los principios de la función electoral y a los del voto y que, derivada de esa legislación, existía una facultad de regulación de la autoridad administrativa que le permitía habilitar el voto por Internet. En tres apartados (que retomamos del modo en que aparecen en la sentencia), la Sala Superior estudió los puntos sustantivos sobre la legitimidad del VPI y las cuestiones constitucionales y legales relacionadas con él.

i. **El primer apartado:** *"Violación al principio de certeza, porque se omitió dar intervención a los partidos políticos al aprobarse como mecanismo de voto de los ciudadanos del Distrito Federal residentes en el extranjero el internet, así como por haber aprobado dicho sistema sin que previamente se hayan llevado a cabo pruebas relativas a la viabilidad y seguridad de dicho sistema de votación".*

La base para declarar la constitucionalidad y legalidad del VPI fue que el Consejo General del IEDF está facultado a aprobar y autorizar los mecanismos necesarios para promover y recabar el voto en el extranjero, de acuerdo al Código de Instituciones y Procedimientos Electorales del DF (en su artículo 57):

> "Asimismo, de la normativa expuesta se desprende que, a diferencia de la legislación federal, no se estatuye de forma expresa que el voto de los ciudadanos del Distrito Federal residentes en el extranjero, para la elección de Jefe de Gobierno, debe ser postal. En efecto, en la ley electoral del Distrito Federal no se prevé alguna modalidad específica para recabar el voto de los ciudadanos de dicha capital que residan en el extranjero, y seguramente por ello, tampoco regula en mayor medida tal clase de sufragio, por lo que se infiere que el legislador local dio

libertad al Consejo General del Instituto Electoral del Distrito Federal para que, con auxilio del señalado Comité, analizara distintas alternativas que permitieran garantizar el derecho del voto a dichos ciudadanos y escogiera la que estimara pertinente, aprobando la normativa, los mecanismos, documentos y demás insumos que se requirieran para ese fin, todo lo cual no tiene que llevarse a cabo, necesariamente, en un solo momento o mediante un acuerdo único, ya que no hay norma que así lo disponga.

Por tanto, debe considerarse que el procedimiento para obtener en forma efectiva el voto de los ciudadanos del Distrito Federal residentes en el extranjero para la elección de Jefe de Gobierno, es un conjunto de actos sucesivos y concatenados entre sí, no aislados, en donde el anterior sirve de base al subsiguiente, llevados a cabo, tanto por el Consejo General, que tiene el carácter de órgano normativo o decisorio, y el Comité precisado, en su calidad de órgano técnico propositivo."

Según la Sala Superior, dado que el legislador dejó una cláusula vaga y abierta sobre las modalidades de la votación, entonces cualquier tipo de votación, tanto la postal como la electrónica, era posible. El argumento descansa claramente en la idea de que la voluntad del legislador y el principio de universalidad del voto se posicionan por encima de otros principios constitucionales.

"Además, **la secrecía se manifiesta en dos principales etapas;** la primera con el hecho de solicitar la contraseña que es única y que se asigna de manera aleatoria, sin conocimiento de algún funcionario público, sino a través de un sistema cifrado que no permite identificar al ciudadano con ésta; y en segundo término, cuando el ciudadano realiza la votación, ya que el voto se transporta por la red a través de un algoritmo cifrado con altos niveles de seguridad que no permite identificar los datos personales del ciudadano con su elección y tampoco el sentido de su voto.

Con lo anterior, la autoridad electoral administrativa estableció la viabilidad de dicho mecanismo de voto, en tanto que, expuso las consideraciones de hecho y de derecho en que apoyó su decisión de implementar el internet como mecanismo de recepción del voto, por lo que era innecesario que antes implementar dicho sistema, hiciera pruebas tendientes a demostrar su viabilidad.

En efecto, **no resultaba necesario que el Instituto llevara a cabo pruebas de desempeño, de estrés o relacionadas con la seguridad en la recepción de la votación, en forma previa a que aprobara el internet como mecanismo para recabar el voto, ya que éstas son meramente técnicas, tendentes a corroborar que el sistema operativo que se escoja funciona en los términos debidos (como podría ser, por ejemplo, que la capacidad de la computadora y el ancho de la banda son los adecuados), y no así para determinar si el mecanismo de internet es apto para garantizar el derecho de voto de los ciudadanos del Distrito Federal residentes en el extranjero, pues esto último, el Instituto Electoral del Distrito Federal ya lo determinó, con base en los argumentos antes expuestos.**

Es razonable que previamente a la realización de las pruebas de un sistema de votación que tiene carácter inédito se proceda a su aprobación, porque así lo exige una cuestión presupuestaria y por que el hecho de que se apruebe la implementación de un sistema de votación, no significa que se deba tener como una determinación pétrea, no modificable o no susceptible de revisión, sobre todo cuando se advierta que tenga deficiencias que deban corregirse o ajustarse a efecto de garantizar la vigencia de los principios rectores de la función electoral y la prevalencia de las características del voto, entre otros principios constitucionales.

En efecto, si el Consejo General del Instituto Electoral local tienen una facultad normativa y resolutiva, a partir del dictamen, o bien, los datos o información que le proporcionara el Comité técnico respectivo, está habilitado para aprobar el acuerdo y procedimiento respectivo, el cual puede modificarse en función de proteger, de la mejor manera, el ejercicio del derecho de voto activo por los ciudadanos del Distrito federal residentes en el extranjero, así como el desarrollo de todas y cada una de las etapas del procedimiento.

La suficiencia presupuestaria y la programación de las actividades, en especial, las pruebas de funcionamiento de la votación por internet, en términos de lo previsto en la normativa respectiva (artículos 51 de la Ley de Presupuesto y gasto Eficiente del Distrito Federal, así como 21 y 22 de las Normas Generales de Presupuesto y Contabilidad del Instituto Electoral del Distrito Federal, los cuales se citaron), justifican plenamente la determinación asumida por el Instituto Electoral local.

En todo caso, para el supuesto de que el sistema no garantizara las condiciones suficientes para asegurar la vigencia de los principios rectores de la función electoral y las características del voto, es susceptible que, además de que se modifiquen los acuerdos relativos para su ajuste y corrección, que también opere el sistema de control jurisdiccional local y, eventualmente, el federal.

Por tanto, no le asiste la razón al tribunal responsable al establecer que dichas pruebas las debió realizar la autoridad administrativa electoral, en forma previa a que aprobara el internet como mecanismo para recabar el voto." [121]

Es muy notorio que para la Sala Superior la aprobación normativa viene primero que la determinación técnica de la seguridad del sistema. En ninguno

121. Resulta interesante, al menos, ver que en su voto disidente, el Magistrado Flavio Galván Rivera sostuvo que la decisión de la mayoría era incorrecta pero porque el CGIEDF no tenía facultades para establecer el VPI, ya que éstas correspondían a la Asamblea Legislativa del DF, rechazando que existiera esa posibilidad para el voto en el extranjero si éste no era previamente legislado:

> "No desconozco que la aludida autoridad electoral también puede regular lo relativo a la utilización de sistemas electrónicos para que los ciudadanos emitan su voto, pues tal norma se debe interpretar de forma textual y de forma sistemática con la demás disposiciones del propio Código, que prevén la exigencia de que este mecanismo sea usado solamente en las secciones electorales previamente determinadas por la propia autoridad, es decir, mediante la instalación de "urnas electrónicas" o cualquier instrumento de esta naturaleza, en las casillas electorales instaladas en determinadas secciones del Distrito Federal.
> En consecuencia, como ha quedado precisado, el Consejo General del Instituto Electoral del Distrito Federal, en mi concepto vulneró el principio de legalidad, al ejercer atribuciones que no le han sido conferidas por el legislador local, al implementar como mecanismo de votación el internet."

de los puntos sustantivos (y esto se mantiene a lo largo de la sentencia) las y los magistrados advierten las complejidades inherentes a los sistemas de votación ni cuestionan los riesgos del cifrado ni del uso del correo electrónico para el procedimiento de voto por Internet, ni tampoco los que presenta el almacenamiento de datos y el uso de servidores para la jornada electoral.

El Tribunal comete una falacia de petición de principio porque presupone que el mecanismo de voto es seguro a *priori* (recordemos su argumento sobre la analogía con los sistemas bancarios en Internet) y para justificar su decisión se apoya en el acuerdo y el anexo técnico que dicen que esto es así. El problema de este razonamiento es, por decirlo coloquialmente que, al "poner la carreta delante de los caballos", el Tribunal presupone lo que debería probar: que el sistema que funciona con los mecanismos de seguridad similares a los de los bancos en Internet es seguro para garantizar los principios democráticos.

Al relegar el análisis técnico de los riesgos de seguridad en concreto, el Tribunal resolvió por separado la cuestión normativa de si, en teoría, el VPI puede ser satisfactorio para garantizar el voto y la legitimidad de las elecciones, cuando lo que debió haber hecho era demostrar si los riesgos técnicos del SEI ponían en riesgo los principios constitucionales que estaban en juego.

ii. **El segundo apartado:** *"Violación al principio de certeza porque en el acuerdo impugnado no se prevé algún sistema que permita establecer que el emisor del sufragio es el titular del derecho."*

El Tribunal Electoral justificó la reglamentación del VPI de forma administrativa por el hecho de que no hay una prohibición expresa en la Constitución que diga que todas las votaciones deben ser presenciales. Partiendo de la premisa de que los sistemas jurídicos están compuestos no sólo por reglas sino también por principios, hizo una interpretación diciendo que los principios constitucionales permitían, en este caso y de forma excepcional, habilitar la modalidad del VPI.

> Para arribar a la anotada conclusión, se tiene presente que los ordenamientos jurídicos no están compuestos exclusivamente por reglas (normas provistas de una estructura condicional hipotética, con un supuesto de hecho y una sanción bien determinada, cuya forma de aplicarlas es la subsunción), sino también por principios, que son mandatos de optimización, que ordenan que algo sea realizado en la mayor medida posible.

> El constituyente estatuyó en el artículo 41 de la Carta Magna, que los partidos políticos tienen como fin promover la participación del pueblo en la vida democrática, contribuir a la integración de la representación nacional y como organizaciones de ciudadanos, hacer posible el acceso de éstos al ejercicio del poder público, de acuerdo con los principios, programas e ideas que postulan, mediante el sufragio universal, libre, secreto y directo.
>
> [...]
>
> Si bien en nuestro país, la forma ordinaria de ejercer el sufragio, para elegir a los titulares del poder ejecutivo, así como a los integrantes del poder legislativo, tanto a nivel federal como local, es de forma presencial, en la que el elector sufraga directamente ante una mesa receptora de votos integrada por un grupo de ciudadanos escogidos al azar. Lo cierto es que, la Constitución General de la República no estatuye que necesariamente las elecciones tengan que ser presenciales, de lo que es válido concluir que **pueden existir casos excepcionales, como el de los connacionales que residen en el extranjero, en los que el ejercicio del voto no se lleve a cabo de forma presencial, sin que ello se traduzca en una violación al voto universal, libre, directo y secreto.**
>
> [...]
>
> Con base en lo expuesto, es factible afirmar que en **casos excepcionales, como tratándose del sufragio de connacionales en el extranjero, que viven en muchos lugares del mundo, el voto no presencial, como lo es el electrónico por internet, puede considerarse como un sistema válido para recibir el voto de los ciudadanos residentes en el extranjero, sin necesidad de mecanismos con cámaras web o lectores de datos biométricos, ya que con ciertos mecanismos de seguridad así como con claves electrónicas para identificar al elector, se cumpliría, con los mencionados principios."**

La Sala Superior acepta el VPI para el caso de los electores en el extranjero, por ser una circunstancia excepcional y da por hecho que "con ciertos mecanismos de seguridad" puede garantizarse el cumplimiento de los principios del voto en este caso. Su lectura de los principios constitucionales la llevan a exceptuar la autorización expresa del Poder Legislativo para reglamentar el voto, desplazando con esta excepción el principio de legalidad que obliga a que toda medida que pueda condicionar un derecho esté dispuesta de manera expresa y clara en una ley tanto formal como material.[122]

En este mismo apartado el Tribunal revisó las condiciones de idoneidad, necesidad y proporcionalidad que las medidas debían de cumplir para reglamentar el VPI:

> Lo anterior, ya que dicho mecanismo cumple con los requisitos de idoneidad, necesidad y proporcionalidad, como se demuestra a continuación:

122. CIDH. Alegatos ante la Corte Interamericana en el caso Ricardo Canese Vs. Paraguay. Transcritos en: Corte I.D.H., Caso Ricardo Canese Vs. Paraguay. Sentencia de 31 de agosto de 2004. Serie C No. 111, párrs. 72. s) a 72.u)

a) Idoneidad. El internet, como mecanismo de voto de los ciudadanos del Distrito Federal residentes en el extranjero, persigue un fin constitucionalmente válido, que es hacer efectivo el derecho al sufragio de dichos ciudadanos; **es idóneo porque dadas las características de dicho sistema de votación, de acuerdo con las conclusiones** del "Estudio comparativo, análisis operativo y técnico de la modalidad o modalidades para recabar el voto de los ciudadanos del Distrito Federal residentes en el extranjero para la elección de Jefe de Gobierno de 2012", que obra en autos, elaborado por el Instituto Electoral del Distrito Federal, y que no fue cuestionado por las partes, ayuda a extender la cobertura del electorado en el exterior, ya que permitiría que un mayor número de capitalinos residentes en el extranjero vote para la elección de Jefe de Gobierno en dos mil doce, sin que ello implique el pago de alguna tarifa postal o la necesidad del elector de desplazarse a algún lugar determinado. Además, por sus características y con la tecnología adecuada de seguridad, permite que se cumpla que el sufragio se emita en forma personal, secreta y directa desde cualquier parte del mundo.

b) Necesidad. El internet, como mecanismo de voto de los ciudadanos del Distrito Federal residentes en el extranjero, es necesario porque de acuerdo con el estudio citado, ayudaría a extender la cobertura del electorado en el exterior, ya que permitiría que un mayor número de capitalinos residentes en el extranjero, vote para la elección de Jefe de Gobierno en dos mil doce, cumpliéndose con el principio de universalidad del voto.

c) Es proporcional, porque dadas las características de los sufragantes, en cuanto a que residen en el extranjero y ordinariamente es difícil que en diversas partes del mundo se instalen mesas receptoras de voto, **los posibles riesgos a las características del voto (libre, secreto y directo) serían mínimos ante el cúmulo de las medidas de seguridad establecidas por la autoridad administrativa electoral,** y mayores los beneficios obtenidos, al lograr una mayor participación ciudadana.

El análisis del test tripartito que hace la Sala Superior es preocupantemente deficiente y tiene problemas en cada uno de los elementos que se supone debería revisar. A grandes rasgos, nos dice que la idoneidad se cumple porque permite que más personas voten en el extranjero y porque es una medida más simple y efectiva para hacerlo; la necesidad se alcanza porque satisface el principio de universalidad al extender la cobertura del sufragio (sin decir mucho más al respecto); y la proporcionalidad porque ante la dificultad de instalar mesas receptoras de voto, aumentar la participación compensa los riesgos a la secrecía y a la vulnerabilidad, haciendo un claro balance de costo beneficio. Pero el análisis de idoneidad, necesidad y proporcionalidad exige mucho más que esto.

El elemento de idoneidad significa que la medida alcanza de manera efectiva el objetivo que persigue o que resuelve el problema en cuestión. El elemento de necesidad exige que la medida que se elige para perseguir ese objetivo o resolver ese problema n*o pueda lograrse por otra medida menos restrictiva*;[123] es decir, que siempre debe usarse la medida menos gravosa o riesgosa para el derecho en cuestión. El elemento de proporcionalidad requiere que la afectación al derecho no debe ser excesiva frente a los resultados que persigue; que debe haber una relación proporcional entre la afectación y el beneficio obtenido.[124]

El problema de la Sala Superior con su análisis de idoneidad es que toma la palabra del IEDF por sentada sin hacer un análisis sustantivo del sistema. Si el estudio era incorrecto o incompleto en términos jurídicos o técnicos no podemos saberlo porque el tribunal esquivó su obligación de revisar la cuestión de forma sustantiva. Un segundo problema es que da por sentado el argumento del aumento de la participación, como si hubiera una certeza absoluta sobre la misma, cuando desde hace años y en esa época ya existían estudios serios que refutaban (o cuestionaban al menos) el mito de la relación causal del VPI y la participación. Un tercer problema es que ni siquiera realiza un análisis sobre si el voto por Internet puede, efectivamente, cumplir lo que promete. Así, la Sala Superior pasa por encima la cuestión sustantiva de determinar si un sistema que puede ser manipulado y que puede poner en juego la legitimidad de una elección, puede en verdad considerarse idóneo sólo porque permite a las personas votar desde casa.[125]

123. Corte IDH. Caso Herrera Ulloa Vs. Costa Rica. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 2 de julio de 2004. Serie C No. 107. Párr. 120-123; Corte IDH. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5. Párr. 46.

124. CoIDH. Caso Herrera Ulloa vs. Costa Rica. Excepciones preliminares, Fondo Reparaciones y Costas. Sentencia de 2 de julio de 2004. Serie C, N.º 107, Párr. 121; Caso Gomes Lund y otros ("Guerrilha do Araguaia") Vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 24 de noviembre de 2010; y Caso Claude Reyes y otros Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 19 de septiembre de 2006. Serie C No 151.

125. En la Parte I del trabajo explicamos con detalle cómo todos estos argumentos son disputados y existe mucha evidencia apuntando en sentido contrario a lo que sostuvo el TEPJF. Ahí también señalamos lo importante de entender que los argumentos deben analizarse sistemáticamente y no por separado, porque su validez es multifactorial; es decir, que depende de que otras cosas se cumplan para poder concluir que un argumento efectivamente es correcto. Por ejemplo, aumentar la participación no depende sólo de que sea más cómodo votar en casa, sino de que la gente confíe en el sistema, de que no haya coerción en el hogar, de que sean capaces de utilizarlo, etc.

El problema con el análisis de la necesidad es que, literalmente, no hay un análisis de la necesidad. La Sala Superior sólo dice que el VPI "es necesario para aumentar la cobertura del electorado en el exterior" y para cumplir con la universalidad del voto. Pero el principio de necesidad no consiste en enunciar que una medida puede parecer necesaria para lograr algo (no se trata de decir solamente que A es un medio para alcanzar B). Por el contrario, la condición de que una medida sea necesaria exige que los jueces demuestren que la medida elegida para cumplir el objetivo (en este caso para aumentar la participación) es la menos riesgosa, gravosa o restrictiva para el objetivo perseguido. Este análisis es inexistente en la sentencia; la Sala Superior no evalúa, por ejemplo, al voto por Internet frente al voto postal (que era lo mínimo esperado en este caso) para determinar que es menos lesivo que el segundo. Simplemente lo da por hecho.

El problema con respecto al análisis de la proporcionalidad es que, primero, da por sentado (nuevamente, sin analizar de fondo el dilema) que los riesgos de este tipo de sistemas son mínimos y, segundo, que el VPI aumenta la participación. Además, parece inferir de sus supuestos que el aumento en el grado de participación es tal que los riesgos que existan (sean los que sean) son compensados en un análisis de costo-beneficio. Un análisis real de la proporcionalidad requería, primero, que las y los magistrados evaluaran los costos en cuanto a riesgos de manipulación del voto, de la elección y violación de la secrecía y, segundo, que evaluaran los beneficios del supuesto aumento de la participación para después llegar a la conclusión de que la medida era (o no) proporcional. La Sala Superior no hizo ninguna de las dos.

Desafortunadamente eso no fue todo. El TEPJF no analizó el problema de la coerción, ni el de los riesgos de los robos de credenciales de usuarios o el del uso de *malware* para cambiar un voto o comprometer una elección. Lo que hizo fue poner la carga de la responsabilidad por la seguridad del voto en las y los ciudadanos, en lugar de evaluar la seguridad de una medida como ésta. Literalmente, la Sala Superior consideró que los riesgos correspondientes al usuario eran "responsabilidad exclusiva del ciudadano" (al menos en cuanto a la custodia de los datos y a la titularidad de quien emitía

el voto).[126] Las afirmaciones hechas reflejan un profundo desconocimiento de los riesgos técnicos y del funcionamiento del ecosistema de Internet. Así, señaló que: "[...] debe considerarse que ordinariamente habrá certeza de que quien vota, es el titular del derecho, porque en principio, sólo quien cuente con la contraseña puede emitir el voto, y esta persona no es otra que el titular del derecho a votar" y que, ante la posibilidad de la coacción y la violación de la secrecía, esos problemas: "no son exclusivos de la votación de tipo remoto, sino que se puede presentar en cualquier tipo de elección".

Las dos afirmaciones son falaces por motivos que a esta altura deberían ser obvios. Primero, porque no sólo es posible sino que una constante de los estudios independientes es que muestran la facilidad y alta probabilidad de que en una elección por Internet un atacante tome control del dispositivo de otra persona y vote por ella sin mucha dificultad. Segundo, porque al decir que la coacción también se da en otras modalidades de votación hace una asociación injustificada: del hecho de que pueda haber riesgos no se sigue que estos sean los mismos ni que existan en el mismo grado o que tengan las mismas consecuencias. El voto por Internet abre un riesgo enorme para la coacción que no existe cuando el Estado está presente: cuando a las personas se les quita ese espacio público donde pueden votar sin nadie que les coaccione, el ejercicio del voto queda condenado a cualquiera que sea el escenario que se vive en la esfera privada, pero esta consecuencia es responsabilidad directa del Estado. Una vez más, no hay ningún análisis sustantivo al respecto.

¿Cómo podemos saber que un mecanismo así es necesario y que es proporcional si no demostramos que efectivamente es seguro y si no mostramos que sus riesgos son menores que los de las otras alternativas

126. La Sala Superior dice claramente que: "a) El correo electrónico que envía el Instituto Electoral del Distrito Federal, tiene como destino una cuenta de correo que el ciudadano solicita el registro en la Lista Nominal de Internet, **de tal manera que es el titular del derecho al voto quien custodia la información relativa a dicha cuenta de correo, siendo responsabilidad del mismo proteger la información que recibe en la misma.**
b) El correo que remite el Instituto Electoral del Distrito Federal, contiene un enlace que solicita información personal, además de la clave de elector, por lo que, aunque en principio, sólo el titular de la cuenta de correo es quien tiene acceso a la misma, **en caso de que otra persona ingresara, necesitaría contar con los datos referidos para continuar con el procedimiento para obtener la contraseña, mismos que son de carácter personal y cuya custodia compete al propio ciudadano**...
d) La custodia de los datos proporcionados por el Instituto Electoral del Distrito Federal **son responsabilidad exclusiva del ciudadano, sin que la responsable tenga injerencia en ello.**"

disponibles? ¿Puede lograrse lo que buscamos por otros medios menos restrictivos (el voto postal, por ejemplo)? ¿El supuesto beneficio del aumento de la participación política era proporcional al riesgo de votar por Internet? Es muy difícil responder estas preguntas cuando no hay un estudio sustantivo para responderlas; cuando en vez de analizar si la seguridad y secrecía se cumplen, se da por hecho que sí; cuando, en vez de demostrar que la participación política aumenta, simplemente se da por sentado (sin siquiera compara con su alternativa, el voto postal)

Paradójicamente, de las pocas medidas que analizó en sustancia, la Sala Superior concluyó que varios de los elementos que hoy en día se usan en el SEI del IECM serían desproporcionales, excesivos y poco razonables. Al analizar otro tipo de medidas de seguridad complementarias tales como el uso de datos biométricos o dispositivos con cámara web, la Sala Superior señala lo siguiente:

> **"No son idóneos ni proporcionales, al ser excesiva y poco razonable, la exigencia de que los votantes cuenten con los requerimientos técnicos necesarios, esto es, con equipos de cómputo que tengan lectores ópticos o dactilares, para poder emitir su sufragio.** El Tribunal Electoral del Distrito Federal no establece cuáles son los datos jurídicos y fácticos que demuestren o desvirtúen la viabilidad y razonabilidad del sistema de votación por internet y, **en forma dogmática, asume que dichos sistemas biométricos o que precisan de fotografías o huellas dactilares (que parecen excesivos o desproporcionados) son infalibles.** No se destruye la presunción de validez del acto de autoridad administrativo. **Asimismo, tales requerimientos no son necesarios, porque como se mencionó, existen otras medidas de seguridad que resultan razonables y buscan en la mayor medida posible proteger las características del sufragio,** pues, en el caso concreto, se parte de la base de que, en principio, sólo quien cuente con la contraseña puede emitir el voto, y esta persona no es otra que el titular del derecho a votar."

A diferencia del (mal) análisis anterior sobre el sistema en general, en este caso la Sala Superior al menos se detiene para realizar una evaluación somera sobre la necesidad y la proporcionalidad. La paradoja es que hoy el IECM presume como avances y medidas de seguridad precisamente las que el TEPJF rechazó en la sentencia que analizamos (el reconocimiento facial para la autenticación de los votantes en la App de su sistema de VPI). El Instituto Electoral es entonces selectivo en el uso de la sentencia, ignorando las partes de ella que están en tensión con su diseño actual y tomando las que le sirven para avanzar sus argumentos.

iii. El tercer apartado: *"Ponderación de principios y urna electrónica"*

El tercer punto de la sentencia muestra claramente que la Sala Superior no consideró necesario justificar si había un método menos riesgoso para la emisión del voto, ya que para ella bastaban las razones dadas por el Consejo General del IEDF:

> "Igualmente en los acuerdos identificados en el párrafo anterior, contrariamente a lo que sostiene la responsable, se precisan las razones por las cuales, además del postal, se optó por el sistema de votación por internet. Esto es, sin desconocer que la responsable no tiene por qué motivar las razones por las cuales no se eligen otros sistemas de votación distintos del postal o por internet para los ciudadanos del Distrito Federal residentes en el extranjero, porque es suficiente con que el Consejo General del Instituto Electoral local precise puntualmente las razones jurídicas y técnicas que le llevaron a optar por un sistema o sistemas de votación para tales efectos y que tales consideraciones sean razonables".

Para la Sala Superior, la ponderación del TEDF fue incorrecta porque no evaluó bien los incisos A y B, en los que se alegaba la violación a los principios electorales y del voto. El TEDF había partido de premisas equivocadas y su ponderación había sido incorrecta, ya que la certeza del voto no resultaba afectada en realidad. Como el Consejo General del IEDF había aprobado el acuerdo en el que establecía el voto por Internet, dando las razones jurídicas y técnicas (en considerandos 25 del acuerdo ACU-47-11 y 33-39 del acuerdo ACU-69-11), la Sala Superior consideró que esas eran razones suficientes para no hacer el análisis y apegarse a las palabras del Consejo.

Más adelante, al ver el "Registro y sistema de entrega de contraseñas", el TEPJF analizó el esquema de mails, contraseñas y *links* utilizados en el SEI para decir que eran suficientes para garantizar los principios del voto. Al hacerlo, volvió a comparar el VPI con los sistemas de compras y de banca por Internet:

> "Lo anterior debe considerarse como un candado, es razonable e idóneo para garantizar la emisión del voto de acuerdo con los principios de universalidad, libertad y secrecía, ya que la solicitud, registro y entrega de contraseña, se realiza a través de un procedimiento automático, el cual, debido a sus características técnicas, presupone objetividad e imparcialidad, pues el mismo opera sin utilizar algún tipo de criterio o mecanismo que lleve a una selección o depuración arbitraria, ilegal o injustificada de los ciudadanos que hayan cumplido con los requisitos legales para votar desde el extranjero. En particular, **debe enfatizarse que, a través de dicho sistema, se garantiza la secrecía del voto, ya que la contraseña con la que se efectuará el sufragio, únicamente, podrá ser conocida por el ciudadano que se registró.**

> Aunado a lo anterior, esta Sala Superior, a partir de las reglas de la experiencia y la lógica, estima que **el sistema cumple con estándares suficientes de seguridad, ya que su funcionamiento es similar al que se utiliza en otros sistemas de internet para accesar a sitios electrónicos que requieren altos niveles de seguridad y confianza, como es la banca en línea o el procesamiento de compra de diversos productos,** en el cual se proporcionan los datos de una cuenta de banco o una tarjeta de internet, en cuyos casos, las claves de acceso son personales y de responsabilidad de su titular, como sucede en el caso que se analiza."

Estos dos párrafos son muy interesantes para la crítica que hacemos a la sentencia por varias razones: primero, porque muestran que la Sala Superior *presupone* cosas del sistema técnico para concluir que no se afectan los principios elementales del VPI; segundo, porque se amparan en *las reglas de la experiencia y la lógica* para decir que los estándares de seguridad son suficientes y luego respaldan la analogía de seguridad con los sistemas bancario y comercial en Internet.

Las reglas de la ciencia computacional no son las mismas que las de la experiencia y la lógica, precisamente porque se trata de sistemas complejos que no permiten dar por sentado lo que los magistrados dieron por sentado. El problema es que este caso debió incorporar esos criterios para poder juzgar la materia del asunto correctamente. Lo más grave es que el Tribunal ni siquiera parece percatarse de que los sistemas que señala como sustento para presuponer su análisis son altamente falibles:

> "Basado en lo anterior, esta Sala Superior arriba a la convicción de que el sistema de voto por internet cuenta con los elementos, medidas y candados de seguridad suficientes, a efecto de que el ciudadano pueda emitir su voto de manera universal, libre, secreta y directa, **ya que la configuración del mismo permite advertir que únicamente el ciudadano registrado que cumplió con los requisitos y recibió la contraseña, podrá entrar al sistema de votación electrónica, y tener acceso a la boleta virtual.**
>
> [...]
>
> Asimismo, el sistema de encriptamiento de la información, el cual permite que la misma sea resguardada en la urna virtual, sin que nadie pueda conocer la información, **permite generar la seguridad y la certeza suficiente,** para garantizar que el sufragio emitido por cada uno de los ciudadanos que se encuentren en la Lista Nominal de Electores del Distrito Federal residentes en el extranjero, será debidamente salvaguardado y en su momento contabilizado.
>
> **Las medidas de seguridad y candados adoptados por la autoridad administrativa electoral son idóneas, ya que sólo pueden tener acceso a la información**

> **quienes cuenten con la llave electrónica que el propio sistema genere, la cual se dividirá en siete partes, de forma que cada uno de los consejeros electorales contarán con una de ellas."**

Al igual que en los puntos anteriores, la Sala Superior no hace un test para ponderar o evaluar la legitimidad de las medidas, sino que establece por definición que el sistema es seguro. Una y otra vez, de manera sistemática, el tipo de argumentación del TEPJF utiliza premisas que deberían ser, en todo caso, conclusiones, para después sostener que las conclusiones a las que llega son lógicas.

Si contrastamos la decisión de la Sala Superior con el modelo que planteamos, es notorio que no cumple con el análisis sustantivo de la primer condición que requiere analizar si el sistema en cuestión puede garantizar la integridad, la secrecía y la libertad del voto (la sentencia, ni analiza los requisitos de la integridad ni advierte los riesgos del lado de los usuarios del sistema ni toma en serio el problema de la coacción del voto); tampoco hace ningún análisis relativo con las implicaciones de contar con un sistema electrónico que funciona de forma poco transparente frente a los principios rectores de las elecciones (principalmente el de transparencia y el de máxima publicidad); y, finalmente, realiza un análisis de las características de idoneidad, necesidad y proporcionalidad que es, por momentos conceptualmente erróneo, por momentos superficial.

b. Sentencia TEDF-JEL-017/2013: el argumento de la promoción del interés de la ciudadanía y la participación política

Otra sentencia en la que el IECM y los impulsores del voto por Internet suelen apoyarse es el fallo en el que el Tribunal Electoral del Distrito Federal resolvió una impugnación en contra del SEI, para recabar el voto y para recibir las opiniones en las elecciones de los Comités Ciudadanos y Consejos de los Pueblos en el año 2013, así como en la Consulta Ciudadana en materia de Presupuesto Participativo del año 2014. En la parte que interesa a este estudio el Tribunal estableció el siguiente criterio:

> "... para este órgano jurisdiccional es indudable que el establecimiento de métodos electrónicos de votación para las próximas elecciones en materia de participación ciudadana, evidentemente tienden a fomentar el interés de la ciudadanía en este

> tipo de ejercicios democráticos, toda vez que su implementación tiene como finalidad, facilitar el ejercicio del voto a los habitantes de esta entidad, a través de la utilización de un mecanismo que en la actualidad se considera de fácil uso para todos los ciudadanos, como es el acceso a una computadora con conexión a Internet."

Es un misterio por qué para el Tribunal es "indudable" que los métodos electrónicos de votación en esas elecciones tienden a fomentar el interés en los ejercicios democráticos. Si bien es cierto que el Tribunal nos dice que siguen el fin de facilitar el voto porque utilizan dispositivos de fácil uso como una computadora conectada a Internet, en esta ocasión el órgano jurisdiccional tampoco entra al fondo de la cuestión y da por supuesta la idea que vincula el uso de las tecnologías y el aumento de la participación de manera causal.

c. Sentencia TEDF-JEL-045/2016

En este caso, el TEDF retomó los argumentos que se utilizaron en la sentencia de la Sala Superior del TEPJF, para decir que el SEI podía garantizar los principios de certeza y seguridad. El IECM hace lo mismo que el TEDF después, para decir:

> "Que en la sentencia emitida por el Tribunal Electoral del otrora Distrito Federal en el Juicio Electoral con clave TEDF-JEL-045/2016, se señaló entre otras cuestiones que el SEI, cumplía con los principios de certeza y seguridad, así como que dicho sistema está diseñado para garantizar las características del voto".[127]

Tanto esta decisión como las anteriores repiten el mismo error metodológico en dos partes. Primero, repiten hasta el cansancio ideas sin sustento ni justificación (sobre la participación, sobre la seguridad, sobre la secrecía) y nunca entran a analizar en sustancia si esas ideas en verdad se cumplen en la práctica (por ello señalamos que parten de presupuestos o premisas que dan por hecho, sin comprobar). Segundo, se apoyan en otras ideas que son abiertamente incorrectas (por ignorancia o desinterés) para completar sus argumentos, tal como sucede con la idea de los sistemas bancarios en Internet y el voto.

127. IECM. (Acuerdo IECM/ACU-CG-014/2017), párrafo 28; exactamente en el mismo sentido ver: IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación*, julio de 2017, p. 29.

Si hay una tendencia que se sigue y repite en las decisiones jurisprudenciales sobre el voto por Internet en México es la del desconocimiento técnico y especializado sobre las tecnologías y el funcionamiento de los derechos en el entorno digital. Desde ahí, una sentencia equivocada ha servido para justificar otras y, el conjunto, para justificar las decisiones administrativas que avalaron establecer el VPI en primer lugar.

d. El Comité Técnico del Instituto Electoral del DF

El Comité fue creado por el IEDF para preparar la elección de Comités Ciudadanos y de los Pueblos 2016 y la Consulta Ciudadana Sobre Presupuesto Participativo 2017, principalmente para emitir opiniones sobre las pautas de seguridad con miras a evaluar el cumplimiento del principio de "una persona, un voto". En su integración también participó una representación de la OEA.

Lo primero a señalar es que no es claro si todas las etapas de implementación del SEI fueron verificadas en detalle por el Comité, ya que parece que su revisión se enfocó solamente en ver si el SEI **era adecuado y confiable en cuanto a su uso** para estos ejercicios participativos (otra vez) en términos funcionales. En algunos lugares, incluso, hay señalamientos explícitos de que "no se hicieron revisiones a aspectos más profundos de su constitución", lo que da la impresión de que su estudio fue más bien superficial y parcial. En este sentido (el subrayado es nuestro):

> Los datos que aportó el paquete documental revisado, muestran que **las principales etapas de implementación, fueron verificadas en detalle por equipos imparciales y altamente especializados.**
>
> Se constató que, en todas las etapas, los protocolos de verificación y de preparación técnica de los lenguajes de programación, equipos físicos e infraestructura, configuraciones informáticas y revisiones de auditoría y de seguridad del sistema fueron adecuadamente aplicados, dejando de todo ello constancia verificable.
>
> Cabe aclarar que **al ser el propósito del análisis dar constancia de que el SEI es adecuado y confiable para ser usado en los ejercicios democráticos de consulta ciudadana y votación comicial, no se hicieron revisiones a aspectos más profundos de su constitución,** sin embargo la constancia que aportan los reportes que realizaron los equipos especializados en diversas etapas de construcción de la solución, avalan en la opinión de este equipo: que el SEI, es un sistema robusto, bien elaborado y cuidado en sus aspectos más significativos.

> Referente a los argumentos presentados por organizaciones ciudadanas y partidos políticos, resalta que no se encontraron elementos en el Sistema Electrónico por Internet, del Instituto, que sustenten debilidades técnicas y de procedimientos electorales para afirmar que permite implantar votos distintos a la persona que sufragó, aunque para asegurar la identidad del votante remoto recomendaron el procedimiento presentado en el Análisis de las modalidades del SEI susceptibles de instrumentarse en la elección de comités ciudadanos y consejos de los pueblos 2016 y en la consulta ciudadana sobre presupuesto participativo 2017.[128]

El IECM señala que posteriormente las observaciones realizadas por el Comité fueron implementadas a tiempo para llevar a cabo ambos ejercicios de participación.[129] Sin embargo, también reconocen que el Comité realizó una recomendación técnica consistente en el "Fortalecimiento de Aplicación de Estándares de Seguridad".[130] ¿Qué significa esto? ¿De qué elementos y fallas del sistema hablan? No existe información pública al respecto.

e. Las auditorías

Este apartado es muy importante porque es partir de las auditorías que podemos saber con mayor detalle si el sistema de VPI del IECM cumple con el modelo y con las condiciones mínimas que garanticen la seguridad de las elecciones y del voto (dado que no se permite hacer pruebas de penetración y recompensa ni ingeniería inversa). Las auditorías, junto con el informe externo especializado de este año sirven como las radiografías más claras y recientes sobre el sistema actual.

La LGIPE establece en su artículo Décimo Tercero Transitorio que el SEI debe contar con dos dictámenes de "empresas de prestigio internacional" que certifiquen la "certeza absoluta y seguridad comprobada" del sistema electrónico que se busque emplear. La información pública del IECM nos permitió la revisión de dos periodos de auditorías: primero en el año 2017, donde fueron realizadas una por la UNAM FES Aragón y la otra por la empresa *Grupo Scanda - Kimat: Empresa privada, S.A de C.V.;* y el segundo periodo en el año 2020, donde solamente se auditó el sistema por la UNAM FES Aragón y posteriormente se solicitó un informe experto

128. IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación, julio* de 2017, pp. 28-29.
129. *Ibidiem*, p. 29.
130. IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Jurídica Normativa*, julio de 2017, p. 15.

externo para evaluar el sistema y su funcionamiento en la jornada. Todas las auditorías fueron pagadas de acuerdo a los Lineamientos del IECM. De acuerdo a lo establecido por el IECM:[131]

> Las validaciones que se realizaron al sistema consistieron en probar todos los aplicativos desarrollados específicamente para el SEI en términos de funcionalidad, así como analizar las posibles vulnerabilidades por medio de la ejecución de pruebas de denegación de servicios, de inyección de código malicioso y de acceso a los diversos recursos del sistema informático, con el fin de corroborar que el sistema tiene implementados los candados necesarios para evitar ataques internos o externos a la infraestructura que aloja el sistema y con esto brindar certeza en la seguridad del sistema.
>
> La ejecución de ambas auditorías al Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de México buscó cumplir con los siguientes supuestos:

- Que la integridad de la información se mantenga durante toda la operación del sistema.
- Que la aplicación fue desarrollada con base en lo que se consideran las mejores prácticas de programación a la fecha.
- Que el sistema es seguro y no permite el registro de datos ajenos al proceso de votación.
- Que el repositorio de información del sistema no es accesible por entes externos y sin el uso de los certificados requeridos para tal fin.
- Que la arquitectura de la infraestructura de cómputo y comunicaciones corresponda a las necesidades del sistema.
- Que las versiones y actualizaciones de los sistemas operativos se encuentren estables; acorde a las necesidades del sistema.
- Que existan procedimientos que permitan asegurar los accesos físicos y lógicos a la infraestructura de cómputo y comunicaciones del Instituto.

A continuación desarrollamos los puntos principales de las auditorías del primer periodo y las conclusiones que el IECM tomó de ellas y luego difundió, para después analizar la última auditoría del 2020 y señalar algunos puntos que nos parecen problemáticos.

La auditoría de la empresa KIMAT (2017)

"Mantener la Continuidad del Negocio"
–Lema de la empresa en la portada de la auditoría

131. IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación,* julio de 2017, pp. 36-37.

La primera auditoría señala explícitamente que su revisión "excluye de forma inicial la auditoría al proceso de pre-registro [...] ni el procedimiento para la entrega y generación de las Claves de Voto por Internet a Correos de México".[132] La razón de esto no es clara, pero puede deducirse de otros puntos del documento que es por la limitación de tiempo y recursos que tuvieron para ello.

En su conclusión sobre la "Revisión de Infraestructura Tecnológica del proceso de votación del sistema electrónico por internet (SEI)" la auditoría dice escuetamente, en un solo párrafo (el énfasis añadido es nuestro):

> Esta revisión se compuso de 3 etapas, análisis de vulnerabilidades y pruebas de penetración tipo "caja negra" (solo conociendo la URl/dirección *web*) desde afuera de las instalaciones y redes del IECM, pruebas de penetración tipo "caja blanca" efectuadas durante el simulacro del SEI en las instalaciones del IECM, y pruebas de Negación/Denegación de servicio (005). Durante las pruebas se comprobó la capacidad del SEI para operar ante ataques y pruebas de seguridad internas y externas **de forma aceptable.** Y es un sistema con estándares suficientes de seguridad y **niveles razonables de confianza.**[133]

Sobre este punto, no es claro qué significa que la seguridad de un sistema es "aceptable" ni tampoco qué es un "nivel razonable de confianza" cuando se trata de un sistema para votar en Internet. Tampoco está claro a qué estándares de seguridad se refiere, pero parece que el criterio no se corresponde con la exigencia de la normatividad electoral que demanda una certeza absoluta de los dispositivos y del sistema para votar.

Tal vez el problema más grande es que el contenido del informe es simplemente descriptivo de las acciones que realizaron o debían realizar y dice poco o nada de lo que encontraron en el SEI, de su funcionamiento y de las cuestiones sustantivas de seguridad que serían relevantes para informar a la ciudadanía. El problema se agrava porque, además de esto, la empresa emitió una serie de recomendaciones o "puntos de mejora" del sistema que generan dudas serias sobre el sistema (el subrayado es nuestro):

- Existe una alta dependencia a un factor crítico en el proceso de envíos de SMS y este es responsabilidad de un tercero.

132. KIMAT. *Dictamen de Auditoría para el Instituto Electoral de la Ciudad de México*, 20 de julio de 2017, p. 8. Disponible anexa en: https://www.iecm.mx/www/taip/cg/acu/2017/IECM-ACU-CG-014-2017.pdf.
133. *Idem.*

- De igual forma **existe un riesgo de que algún operador celular interfiera con la recepción de los SMS.**
- **No existe un método o procedimiento para la verificación de respaldos efectuados.**
- Se recomienda limitar o desaparecer el uso de archivos de texto plano o **protocolos inseguros en la transmisión de información crítica.**
- Se recomienda el i**mplantar cifrado para el tránsito y almacenamiento de archivos críticos de la operación.**
- Establecer más de un único punto de contacto para enlace con **los interlocutores y/o terceros que provean servicios de TI.**
- Algunos de los componentes de la revisión técnica fueron descubiertos y al analizarlos se descubrió el uso de cifrado base64 por lo que **se recomienda utilizar un cifrado más robusto.**[134]

Las recomendaciones no explican en qué consisten las fallas sino que simplemente hacen una conclusión en tal o cual sentido. No es posible saber qué error, dónde y de qué gravedad se encontró en el SEI; lo que sabemos es que el sistema contenía errores relacionados con el cifrado del sistema (y que éste no usaba un cifrado suficientemente robusto), que se menciona el uso de "protocolos inseguros en la transmisión de información crítica" y que hay varios elementos que podrían representar vulnerabilidades graves.

Otro problema es el condicionamiento del tiempo (insuficiente) para la revisión. En su conclusión, el informe señala el poco tiempo que tuvieron para realizar la auditoría: "A través del análisis de los hallazgos. la documentación y las pruebas técnicas (**a pesar del corto tiempo permitido para las pruebas**) las características del SEI son perceptibles y entre ellas el autor del documento y el equipo de auditoría listan..." (el énfasis es nuestro).[135] Además, tampoco es claro si la empresa tuvo la posibilidad de revisar el código de manera abierta y completa, así como de realizar ingeniería inversa en el sistema. Frente a estos hallazgos, ¿Qué es lo que el IECM difunde y resalta sobre esta auditoría en sus documentos públicos? Solamente esto:

> **Conclusiones de Grupo SCANDA - KIMAT**
>
> "Habiendo realizado la auditoría correspondiente sobre el sistema de voto electrónico presenta una opción viable para ejercicio democrático del voto. A través

134. *Idem.*
135. *Idem.*

del análisis de los hallazgos, la documentación y las pruebas técnicas (a pesar del corto tiempo permitido para las pruebas) las características del SEI son perceptibles y entre ellas el autor del documento y el equipo de auditoría listan:

- Agilidad en la emisión del sufragio.
- Procesos complejos y funcionales de diseño y operación.
- Rapidez en el conteo de resultados.
- Monitoreo y alertamiento de infraestructura interna y externa.

El evento de simulacro, así como la revisión procedural y de infraestructura se desarrollaron de manera exitosa.

El SEI cuenta con las garantías necesarias para su implementación, y dado que el sistema cuenta con rigurosos controles que garantizan los elementos básicos de:

- Confiabilidad
- Integridad
- Disponibilidad

Es en opinión de Kimat que el sistema SEI es viable, conveniente y puede ser utilizado sin poner en riesgo el respeto a la secrecía del voto/opinión y garantiza el principio de 1 Ciudadano, 1 Opinión, 1 Voto."

La auditoría de la UNAM FES Aragón (2017)[136]

La otra auditoría fue realizada por la Universidad Nacional Autónoma de México a través de la Facultad de Estudios Superiores Aragón (UNAM-FES Aragón). La auditoría señala que sí revisó el código fuente de la aplicación utilizada en el sistema para posteriormente revisar las posibles vulnerabilidades del sistema.[137] Después de especificar esto, dice que al hacer el análisis externo (desde Internet, también llamado de "caja negra") de vulnerabilidades, "obtuvieron hallazgos" sobre éstas y que las reportaron al IECM de manera privada en un "reporte técnico", diciendo que si bien no eran un riesgo "crítico", sí era posible obtener mejores resultados si hubieran contado con un mayor tiempo, haciendo imposible saber los detalles de las vulnerabilidades y evaluar sus implicaciones.

136. UNAM FES Aragón. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, dictamen auditoría UNAM*, julio de 2017. Disponible adjunta en: https://www.iecm.mx/www/taip/cg/acu/2017/IECM-ACU-CG-014-2017.pdf.
137. *Ibidem*, p. 3.

> Los hallazgos que se obtuvieron fueron informados en el reporte técnico sin presentar un riesgo crítico para la utilización del sistema "SEI", **consideramos que se pueden obtener mejores resultados en una ventana de tiempo mayor, brindando un análisis de mayor profundidad,** las vulnerabilidades encontradas básicamente permiten observar alguna información del servidor y de las versiones de las herramientas que se utilizan, si bien esa información no es crítica sugerimos evitar que se muestre.[138] [Énfasis añadido]

Sucede lo mismo con el análisis interno de seguridad (o de "caja blanca"), donde la auditoría es clara en que era posible un análisis de mayor profundidad para detectar vulnerabilidades de una mejor forma, al tiempo que señalan que el estudio podía haber sido mejor si hubieran tenido "los permisos adecuados para su realización", sin especificar a qué se refieren con esto:

> Los hallazgos que se encontraron se documentaron y se emitieron recomendaciones, ninguno de ellos compromete la seguridad de los servidores involucrados, **consideramos que se pueden obtener mejores resultados en una ventana de tiempo mayor y brindándonos los permisos adecuados para su realización y así brindar un análisis de mayor profundidad,** las vulnerabilidades encontradas básicamente permiten observar alguna información del servidor y de las versiones de las herramientas que se utilizan, si bien esa información no es crítica sugerimos evitar que se muestre.[139] [Énfasis añadido]

Las pruebas de denegación de servicio que probaron la infraestructura del SEI se hicieron en un espacio de 60 minutos establecidos por el IECM y la auditoría reconoció que "el volumen de peticiones utilizado en esta prueba no fue de gran escala". Además, las pruebas se ejecutaron teniendo una planeación previa de tan solo 48 horas.

> Los hallazgos encontrados, así como los detalles de la ejecución de estas pruebas fueron entregados a los responsables correspondientes. La organización auditada mostró una infraestructura de red confiable, lo suficientemente robusta para resistir la prueba de denegación de servicio de bajo volumen. **Es importante mencionar que el periodo de tiempo sobre el cual trabajamos la planeación de las pruebas y la ejecución de estas fue corto,** en futuras pruebas se recomienda ampliar el tiempo en el que se planea y realiza la denegación del servicio.[140] [Énfasis añadido]

138. *Ibidem,* p. 9. Aquí es importante recordar que para esta etapa de las pruebas (de caja negra) sólo se les permitió llevar a cabo los análisis en una ventana de tiempo de 60 minutos. De ahí el señalamiento de que podían haber obtenido mejores resultados de contar con un tiempo mayor (ver en página 8).
139. *Ibidem*, p. 10.
140. *Ibidem,* p. 11.

Finalmente, llaman la atención dos últimas observaciones sobre las limitaciones en la realización de la auditoría de partes importantes de la misma:

> Pruebas de estrés a las aplicaciones que se utilicen en el "SEI" identificando así los siguientes umbrales de riesgo: alto, moderado, menor, bajo.
>
> Resultado de la revisión: **Esta prueba no se realizó en esta primera etapa porque el tiempo establecido fue insuficiente para su desarrollo.**
>
> Verificar que el "SEI" contenga un catálogo de errores con su respectiva acción correctiva.
>
> Resultado de la revisión: **No se mostró evidencia**.[141] [Énfasis añadido]

Es preocupante que una de las pruebas para identificar riesgos en el sistema no haya tenido el tiempo de realizarse y que el catálogo de errores no existiera, particularmente cuando tomamos en cuenta que los riesgos de manipulación de una elección y de la ruptura de la secrecía o el fraude electoral por Internet se pueden materializar en un espacio de tiempo mucho mayor al limitadísimo tiempo dado por el IECM. El riesgo se multiplica dependiendo del escenario de riesgo que contemplemos: mientras más poder tenga el atacante (si imaginamos a un Estado o un sujeto con poder económico similar), más probable es romper la seguridad y manipular una elección por completo.

¿Qué es lo que el IECM difundió en el año 2018 en el Acuerdo del Instituto sobre las conclusiones de esta auditoría? (los subrayados son nuestros):

> **Conclusiones de la UNAM - FES Aragón**
>
> "Como resultado de las pruebas y revisiones a la infraestructura y el desarrollo del Sistema Electrónico por Internet ("SE/") del Instituto Electoral de la Ciudad de México, manifestamos que:
>
> - Los servidores e infraestructura asociada a los procesos del ("SEI") son razonablemente seguros, su nivel de riesgo es muy bajo para la operación del servicio mencionado. Sin embargo, se recomienda tener un sitio alterno para elecciones vinculantes.
>
> - El "SEI" del Instituto Electoral de la Ciudad de México es robusto, confiable, y cumple con los requerimientos funcionales del sistema, realiza el 100% de Ias funcionalidades para las que fue creado y no realiza ninguna actividad fuera de las que están descritas en la documentación del sistema.
>
> El sistema "SEI" del Instituto Electoral de la Ciudad de México está en condiciones adecuadas para operar tanto para la consulta ciudadana de presupuesto participativo 2018 como en el voto en el extranjero para la elección de gobernador 2018.

141. *Ibidem,* p. 25.

La auditoría realizada por la UNAM se dividió en tres partes: 1) un informe final sobre el *software*, previo a la jornada (evaluando del 24 de febrero al 30 de marzo de 2020); 2) el informe realizado durante la jornada (evaluando del 7 al 15 de marzo); y 3) un informe posterior a la jornada (evaluando del 15 al 17 de marzo).

- El informe final de *software* (previo a la jornada)[142]

Tal como la auditoría anterior, el objetivo fue evaluar la infraestructura y funciones del SEI para ver posibles riesgos y vulnerabilidades. El estudio analizó la "funcionalidad e inspección de código fuente" y las posibles vulnerabilidades del sistema. También, como en el caso anterior, hubo documentos privados que se entregaron a la Unidad Técnica de Servicios Informáticos del IECM y que no son públicos.[143]

Las pruebas de tipo "caja negra" (casos de prueba para el uso relacionado con el sistema) sistematizaron los riesgos en tres niveles (bajo, medio y alto) según las fallas encontradas, que consisten en qué tan críticos son para el SEI en general. Las pruebas de funcionalidad se dividieron en 22 casos de prueba que tenían "pasos" a seguir que se clasificaban como correctos (el resultado esperado es igual al resultado obtenido), incorrectos (el resultado obtenido es distinto al esperado) e inconclusos (el paso se ejecuta pero no se puede observar el resultado para compararlo con lo esperado debido a falta de información en la base de datos).[144]

La revisión se hizo en dos etapas, una preliminar y una final. De la primera resultaron 185 pasos a probar, de los cuales 111 correspondieron al SEI en los módulos presenciales y 75 al SEI en vía remota. Los primeros tuvieron 5 pasos incorrectos y los segundos 5 incorrectos y 1 inconcluso. En la revisión final no se tuvo ningún paso incorrecto ni inconcluso. El informe no señala cuáles fueron los elementos que tuvieron problemas y sólo señala que no fueron utilizados en la revisión final.[145]

142. UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe final de la Auditoría de Software previo a la jornada de votación y opinión.* Periodo de evaluación: 24 febrero a 30 de marzo de 2020. Disponible en: https://www.iecm.mx/wp-content/uploads/2019/12/SEI_InfFinal2020.pdf.
143. *Ibidem*, p. 3.
144. *Ibidem,* pp. 6-8.
145. *Ibidem,* pp. 9-11.

El análisis de la infraestructura tecnológica evaluó los servidores, las aplicaciones web, los equipos de telecomunicaciones y las estaciones de trabajo. Este análisis también constó de dos fases, en las que se determinó la existencia de vulnerabilidades de cuatro niveles: mínimo, medio, alto y crítico. Aquí encontraron un hallazgo de impacto medio y tres de impacto menor. Tras la notificación al IECM se determinó que el hallazgo de impacto medio era un falso positivo. [146]

La UNAM reportó que en la revisión de las configuraciones de los dispositivos de la infraestructura tecnológica, el análisis sobre los servidores correspondientes al SEI y los dispositivos que los protegen fue "aceptable en cuestiones de seguridad", pero ninguno de dichos hallazgos es mencionado ni explicado, sino que fueron entregados al IECM en el "Anexo Técnico para el sistema SEI 2020", por lo que no es posible saber en qué consistieron ni cuál fue su magnitud. Finalmente concluye que encontraron "servidores con parches de *software* actualizados, con una correcta configuración de seguridad".[147]

En el análisis del código fuente, la auditoría utilizó "dos herramientas que analizan el código y los archivos de la aplicación de manera automática y los hallazgos verificados manualmente". Al hacerlo, la auditoría encontró 42 *bugs* (cosas que están mal en el código) en la evaluación sobre la fiabilidad del sistema (vulnerabilidades) y lo evaluó con el peor nivel (E, que significa que al menos existía un bug bloqueador con probabilidad de impactar en el comportamiento de la *App*; en este nivel la corrección de seguridad como de las buenas prácticas de programación es la más grave), mientras que en el nivel de seguridad se encontraron 53 vulnerabilidades con al menos una de carácter crítico que también requería una modificación y revisión mayor. El código tuvo un 19.7% de duplicado y 1, 286 evidencias de malas prácticas (violaciones) al código encontradas.[148] En sus observaciones y conclusiones:

> Se encontraron varios *bugs* y vulnerabilidades, sin embargo, se revisaron y **la mayoría fueron falsos positivos** ya que se encuentran en archivos generados

146. *Ibidem,* p. 20.
147. *Ibidem,* p. 16.
148. Si volvemos al caso de estudio de EUA, recordaremos que el *hackeo* al sistema de VPI de Washington D.C. consistió en encontrar un error en una línea del código que utilizaba dos comillas ("") en lugar de sólo una ("). Como la evaluación del VPI no es transparente ni independiente no podemos saber, en este caso, si las fallas podían poner en un riesgo similar el sistema de la CDMX. El señalamiento es importante porque el sistema falló en la jornada electoral, no funcionó y tuvieron que hacer un ajuste al código ese mismo día (sin ser auditado). Explicamos esto en detalle más adelante.

automáticamente, algunas otras evidencias encontradas fueron resueltas o tratadas adecuadamente en el mismo código.

Sobre el resto, así como sobre los code smells, se encontraron algunos detalles sobre convenciones de programación que no se siguieron. de este modo, no afectan al funcionamiento del sistema, pero se recomienda seguir las convenciones para que el mantenimiento del *software* sea más sencillo. [149]

La UNAM concluyó que el sistema era seguro y hacía lo que debía hacer y nada más. En el apartado de las conclusiones del dictamen, señaló que los servidores y la infraestructura del SEI eran "razonablemente seguros", y que el sistema era robusto, confiable y hacía el 100% de las funcionalidades para las que lo crearon.[150]

Las conclusiones de la auditoría y los hallazgos en torno al código son preocupantes porque reflejan la imposibilidad de cumplir con los principios de transparencia y de máxima publicidad. Toda la información relevante fue comunicada de forma privada al IECM y no puede ser sujeta al arbitrio público. Además, el análisis del código fuente, al parecer, se hizo de forma semi-automatizada y encontró numerosos errores que podían comprometer el sistema. Si recordamos todas las experiencias de estudios independientes que demostraron la falibilidad y vulnerabilidad de los sistemas del VPI a partir del análisis del código, veremos que la revisión detallada y manual del código es indispensable para detectar errores.

Incluso yendo más allá de este detalle metodológico, el reporte de errores marca un número importante de fallas de las que no podemos saber su nivel de riesgo en caso de que un atacante intentara manipular el código. Este hecho muestra la necesidad de contar con pruebas independientes y expertas de penetración y recompensa, y de la posibilidad de realizar ingeniería inversa en estos casos.[151]

- El informe realizado **durante** la jornada[152] y el informe **posterior**[153]

149. UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe final de la Auditoría de Software previo a la jornada de votación y opinión.* Periodo de evaluación: 24 febrero a 30 de marzo de 2020, p.25.
Ibidem, pp. 25-27.
150. *Ibidem,* pp. 25-27.
151. En la Parte II de esta investigación mostramos cómo en los casos más importantes del VPI, Estonia y EUA, el análisis completo del código fuente y el uso de ingeniería inversa fue lo que permitió a los investigadores desnudar el verdadero riesgo de los sistemas.
152. UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de la Auditoría Informática realizada durante la jornada.* Periodo de evaluación: 7 al 15 de marzo de 2020. Disponible en: https://www.iecm.mx/wp-content/uploads/2019/12/SEI_InfFinal2020.pdf.
153. *Ibidem,* p. 5.

El día de la jornada electoral se llevan a cabo distintos actos que involucran tanto al personal directivo como al personal operativo del IECM y que son la base que hace funcionar el sistema de voto por Internet. El procedimiento, un poco complejo en aras de aumentar la seguridad del mismo, es muy ilustrativo de los riesgos de un sistema de VPI tan solo en lo que respecta a su funcionamiento, por lo que vale la pena ir paso a paso para señalar algunas preocupaciones al respecto.

Uno de los momentos más importantes es el del "Procedimiento técnico de Firma del Código y Configuración del SEI", que permite que la votación remota se lleve a cabo. Para echarlo a andar, es necesario utilizar una **memoria USB** con los archivos del código fuente del sistema para la votación. Es decir, que una persona debe cargar la memoria externa y después entregarla al personal técnico de la UTSI (Unidad de Tecnología de Servicios Informáticos), quienes después realizan una copia de los archivos de la USB y la pasan a una **computadora portátil** (esta acción está a cargo del "Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías"), para después establecer el HASH de los archivos.[154]

Posteriormente, el Secretario Ejecutivo del IECM usa una **nueva USB** con la llave de la elección y luego ingresan el "certificado de la elección" (también a cargo del Jefe de Departamento Web). Hecho esto, el Secretario Ejecutivo ingresa la contraseña de la llave de la elección y el Jefe de Departamento Web selecciona el certificado de la llave de la elección, para después asegurar los archivos de la USB con el certificado de la llave de la elección. Luego, el Secretario Ejecutivo ingresa su contraseña para firmar el código fuente del SEI-2020 (en presencia de parte del personal de la UTSI y de las autoridades del IECM), el Jefe de Departamento Web retira la USB con los archivos firmados de la computadora portátil y la entrega al titular de la UTSI, para después colocar la USB en un sobre, colocar los sellos y entregarlo al titular de la UTSI. Finalmente el Contralor Interno, el Secretario Ejecutivo y el titular de la UTSI lacran el sobre y lo entregan al Secretario Ejecutivo para que lo guarde, mientras que el titular de la UTSI se queda una copia de los archivos binarios.[155]

154. Un HASH es una función criptográfica utilizada para resumir una cadena de información o un bloque de datos a un formato nuevo de caracteres con una longitud finita. La información que es transformada tiene siempre el mismo hash.

155. UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de la Auditoría Informática realizada durante la jornada.* Periodo de evaluación: 7 al 15 de marzo de 2020, pp. 3-4.

¿En qué momento se habilita para votar y cómo funciona la *App* de la votación dentro de este procedimiento? Da inicio cuando el sistema de VPI está abierto. Para votar la electora debe ingresar con la opción de votar, seleccionar la opción de la credencial (para identificarse) y **realizar un escaneo de la parte frontal y el anverso** para corroborar la información de la votante, quien luego debe grabarse en video para verificar que sea la misma persona que la que dice la credencial.

¿Cómo resultó el ejercicio de la jornada electoral una vez que el sistema se echó a andar? El sistema tuvo problemas para funcionar con los dispositivos *Android,* y sus usuarios no podían (y muchos no pudieron) ingresar al sistema. La corrección del problema tomó algunas horas y consistió en **subir una actualización para la aplicación del código** ese mismo día.[156]

> El problema se debió a que mientras en iOS el cambio del escenario de los simulacros al escenario real se realizó de forma transparente en Android se presentó un problema con el manejo de las boletas, **lo cual se resolvió realizando unos ajustes en el código. Es importante mencionar que el sentido de los votos no se vio comprometido.** [157] [Énfasis añadido]

La autoridad modificó el código de la *App* el mismo día, en el mismo momento en que las elecciones se estaban llevando a cabo, con el objetivo de corregir el problema que tuvo lugar. No está claro de qué forma se puede asegurar que el sentido de los votos no se vio comprometido y el reporte no desarrolla este punto en absoluto, pero a esta altura sabemos que cualquier ajuste o modificación al código puede permitir la manipulación total del sistema y poner en riesgo toda la elección (como ejemplifican los casos de Washington y de Estonia analizados más arriba). Justo en este punto hay un problema más preocupante aún. Una vez que la UNAM explica lo que sucedió, señala que:

> Como parte de la auditoría se realizó un análisis forense para verificar las causas del incidente, **las cuales fueron informadas al IECM para que las tome en consideración para el futuro.**[158] [Énfasis añadido]

Esto significa que no podemos saber qué pasó ni cuál fue el ajuste ni mucho menos cuáles son las bases que justifican que la elección no se comprometió. El informe señala que la disponibilidad del sistema no fue la esperada tanto en la versión remota como en la aplicación para iPad, probablemente porque

156. *Ibidem,* p. 9.
157. *Ibidem,* p. 5.
158. *Ibidem,* p. 7.

las pruebas realizadas durante los simulacros "no fueron suficientemente cercanas a las condiciones reales de la jornada", y que no se contó con el "tiempo y recursos suficientes para que se realicen pruebas exhaustivas y que los simulacros se realicen con parámetros muy cercanos a los que se manejarán durante la jornada". Por ello recomendaron tener los requerimientos con suficiente tiempo de anticipación y congelar el diseño a partir del 1er simulacro, del cual los únicos cambios que debería haber son los relacionados con la corrección de errores.[159]

Si ya habíamos señalado el problema de la limitación excesiva del tiempo de las auditorías (y la superficialidad de los análisis en cuanto a seguridad e integridad del sistema) como algo preocupante, es alarmante saber que, probablemente, lo que fue auditado en los simulacros de evaluación fue distinto a lo que se usó en la jornada electoral y que el diseño final con el que se desarrolló la elección también fue distinto. Muchas cosas pueden salir mal en un contexto así porque los riesgos de infectar el sistema aumentan exponencialmente.[160]

El problema del tiempo insuficiente se conecta con otro que desarrollaremos en el apartado siguiente (del informe externo): el de las limitaciones sustantivas de las auditorías frente a los Lineamientos del IECM y los tiempos de la elección. Esto no es raro en los casos de las auditorías de los sistemas de voto por Internet en el mundo. Un argumento alternativo al del tiempo, también para impedir la revisión completa de los sistemas de VPI, es el de la propiedad intelectual, en particular cuando hay empresas involucradas en parte del *software* o el *hardware* con los que se opera un sistema. En este caso:

> Si bien es cierto que en el acuerdo IECM/ ACU-CG-077/2019 se plasman lineamientos que el sistema de voto electrónico deberá respetar, nos hallamos todavía ante un cuadro incompleto ya que los alcances totales de ciertas actuaciones, entre las que se halla singularmente la propia auditoría, no se determinarán hasta que se complete un "instrumento jurídico" entre IECM y la auditora en el que se establecerán:
>
> "I. Los alcances mínimos de la auditoría, establecidos en los presentes Lineamientos y el plan de trabajo asociado al mismo [sic];

159. UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de Evaluación de la Auditoría Informática (informe posterior a la jornada).* Periodo de evaluación: 15 al 17 de marzo de 2020, pp. 7-8.

160. Al analizar el informe experto externo veremos que a los riesgos por el mal funcionamiento se suman otros como el de que la computadora portátil que se utilizó para echar a andar la elección no era de uso exclusivo para la misma, lo cual implica el riesgo de la manipulación de la elección si esa computadora personal estuviera infectada.

II. La información que la autoridad electoral administrativa pondrá a disposición del ente auditor, **salvaguardando en todo momento los derechos de la propiedad intelectual y la protección de los datos personales de las y los ciudadanos"** (art. 50 / Lineamientos).

En el apartado que sigue mostramos que la profundidad del análisis de la auditoría no es clara, ni tampoco si pudieron revisar todos los elementos de seguridad (en algunos puntos es claro que no, y que se enfocaron más en cuestiones de funcionalidad). Es muy común que algunos elementos de seguridad sobre los sistemas no estén sujetos a revisión o lo estén solamente previo acuerdo estricto de confidencialidad, bajo el argumento de defender el derecho de propiedad intelectual. Al menos desde los lineamientos y la práctica del IECM en las auditorías esta posibilidad está abierta, lo que contraviene abiertamente principios rectores de las elecciones tales como la transparencia, la publicidad y la certeza.

Es importante decirlo claramente: hacer lugar al principio de propiedad intelectual en los sistemas de VPI hace imposible garantizar estos principios al mismo tiempo, porque las limitaciones que impone el primero impiden analizar el sistema a profundidad (volviéndose un obstáculo para la publicidad y para la transparencia). Ante esta realidad, quedamos frente a dos caminos que llevan a un mismo lugar: el de creer que lo que nos dicen es cierto aunque no podamos verlo, o el de llegar a un callejón sin salida donde la única opción que nos queda es tener un acto de fe en el sistema. Pero las elecciones no son ni deberían ser un acto de fe.

Finalmente, el sistema de VPI cuenta con un modelo presencial que se hace por medio de iPads en módulos para que la gente vote. Este año esta modalidad se realizó en dos alcaldías completas (Cuauhtémoc y Miguel Hidalgo). La auditoría muestra que desde el momento de inicio se recibieron llamadas denunciando problemas de funcionamiento por falta de señal e imposibilidad de conectarse al SEI. Además, un segundo problema "crítico" fue que en prácticamente todas las terminales se hizo un cuello de botella en los servidores y las terminales que lograban la conexión la perdían posteriormente. El cuello duró dos horas y media y para cuando se mitigó "ya varias mesas habían cambiado de la modalidad electrónica a papel". [161]

161. UNAM FES Aragón Centro Tecnológico Aragón, *Laboratorio de Cómputo. Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de la Auditoría Informática realizada durante la jornada*. Periodo de evaluación: 7 al 15 de marzo de 2020, pp. 18-19.

f. El informe externo final

El último estudio con el que podemos revisar a una profundidad razonable el sistema de voto por Internet es el que el IECM solicitó a expertos independientes en la materia. El instituto pidió un reporte especializado sobre el SEI a dos especialistas externos al Instituto para evaluar su uso en las elecciones de los Comités Ciudadanos y los Presupuestos Participativos de 2020 y 2021.

El proceso de votación tuvo dos etapas de votación, una "anticipada" y la otra final. El periodo de "votación anticipada" duró entre el 8 y el 12 de marzo y hubo algunas demarcaciones en las que el único mecanismo habilitado para votar fue el VPI en los módulos presenciales.[162]

El informe reconoce que no es exhaustivo de todos los trámites necesarios para la implementación del sistema, pero considera que su profundidad permite tener "hallazgos de trascendencia para el conjunto del proyecto". Sus limitaciones se circunscriben a: el registro de ciudadanos que eligieron votar por internet; la firma del código fuente y la configuración del SEI; la votación por internet; la apertura de la urna virtual y el cómputo de votos; la configuración del SEI; el voto por internet en mesas electorales y la carga de la llave criptográfica del SEI. El sistema funcionó en sistemas *iOS* y *Android,* en una aplicación para dispositivos móviles y otra versión de escritorio. Todo por medio del siguiente proceso:

> El votante ingresa datos de su credencial de elector manualmente (clave de elector y OCR), o bien hace una captura de su credencial de elector vía cámara del dispositivo a fin de que se reconozcan automáticamente los datos de la clave de elector y el código OCR. Debido a que actualmente existen tres tipos de credencial de elector vigente, el votante tiene que escoger el tipo de la propia y es apoyado para ello con imágenes de ejemplo de las tres variantes, que son mostradas por la aplicación.
>
> Una vez validados los datos de la credencial de elector, el votante escoge si desea recibir la contraseña de acceso al sistema de votación a través de correo postal o por correo electrónico. Si elige la opción de correo electrónico, tiene que hacer una validación adicional que consiste en tomar algunas capturas del rostro en las posiciones que indica la aplicación. Entonces se realiza un proceso de comparación de la fotografía en la credencial, capturada previamente, con las imágenes del rostro del ciudadano. Dichas validaciones consisten en la toma de medidas de ciertos puntos del rostro como, por ejemplo, distancia de oreja a nariz o distancia

162. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, p. 2.

de oreja a ojo. Si se valida correctamente, la contraseña es enviada al solicitante por correo electrónico; de otra manera, el envío se realiza por correo postal.[163]

Al utilizar la aplicación por teléfono, se guarda la dirección MAC del teléfono para detectar acciones sospechosas, al mismo tiempo de que se registra el número de celular y éste no puede ser usado para registrar a otra persona (sólo puede haber un voto por cada teléfono). Luego se hace un proceso de comparación del rostro por video y se envía la contraseña por email al haber confirmado la identidad. El proceso de análisis del rostro "se ejecuta a través de un *web service* que provee la empresa Ho1a. La aplicación de registro captura las imágenes del rostro y las envía, junto con la imagen de la fotografía de la credencial de elector, a dicho *web service* que, después de realizar la comparación, devuelve un valor estableciendo si hay o no similitud entre la fotografía de la credencial de elector y las imágenes del rostro del solicitante".

En este punto, el informe advierte correctamente que tanto la contraseña del mail como el teléfono inteligente de las personas son vulnerables. La recomendación al respecto es que las contraseñas se cifren con una función hash antes de almacenarse en la base de datos "a fin de evitar que puedan ser conocidas, sea de manera legítima o no, por los que tengan acceso a la base de datos".[164] ¿Qué significa esto?

Primero, que la idea de mitigación de riesgos sobre las contraseñas sigue siendo la de cargar la responsabilidad del cuidado de sus credenciales al electorado. Ya sabemos que el cifrado puede ser burlado de distintas maneras y que el robo de credenciales en Internet es relativamente fácil. Pero un segundo problema es que, en este caso, el procedimiento incorpora a una empresa para la validación de la identidad en el sistema, lo que implica la triangulación de información a través de Internet cada que una persona quiere validar su identidad para recibir la contraseña por mail. En caso de que un atacante tuviera el interés y los recursos para afectar una elección, podría incluso elegir qué punto de ese triángulo atacar para ganar control, violar la secrecía e intentar afectar la elección. [165]

163. *Ibidem,* p. 3.
164. *Ibidem,* pp. 3-4.
165. No está de más mencionar la dificultad de realizar el proceso de verificación y que, de nuevo, éste dependa de un privado que puede ser comprometido o corrompido. En la reunión llevada a cabo el 20 de enero con R3D, uno de los consejeros realizó una demostración de la validación de identidad teniendo que repetir la operación varias veces durante varios minutos (aún conociéndola a la perfección). Las dudas sobre la usabilidad de la aplicación para personas que no son diestras con la tecnología son muy altas en este sentido.

Después está el proceso de firma del código fuente y de la configuración del SEI, en el que se realizan los pasos siguientes:

Se realiza la copia de código fuente de una memoria USB a una computadora personal que no tiene conexión a internet.

Haciendo uso del *software* comercial *Quickhash*, se aplica una función SHA-256 a cada uno de los archivos que componen el código fuente.

El secretario ejecutivo provee la clave criptográfica para realizar la firma digital de los archivos. La clave criptográfica se encuentra almacenada en una memoria USB que resguarda el secretario ejecutivo, quien debe ingresar su contraseña para realizar la firma digital. Este proceso de firma digital se realiza utilizando el *software* comercial llamado SeguriDoc.

Se realiza una copia del código fuente firmado en la memoria USB.

La memoria USB se guarda en su sobre, que es sellado con una cinta de seguridad y posteriormente firmado por el auditor, por el secretario ejecutivo y por el contralor interno del IECM.

El sobre queda en posesión del secretario ejecutivo, quien posteriormente lo lleva a una caja fuerte localizada en su oficina.

Una vez realizado el proceso de firma, se continúa con la configuración del SEI, en donde el administrador del sistema realiza las siguientes actividades:

Se crea la elección, asignándole un nombre, y se especifican las fechas y los horarios de su inicio y fin.

Se realiza la importación de catálogos de la elección: i) ciudadanos que votarán por internet, ii) unidades territoriales, iii) candidaturas y iv) proyectos 2020 y 2021.

Después de la carga de los catálogos, se comprueba, a través de la opción del sistema “Avance de la votación”, que el sistema se encuentra cerrado, ya que debe abrirse automáticamente para la recepción de los votos el primer minuto del día 8 de marzo.

Controles de seguridad en el proceso

El código firmado se almacena en la memoria USB y es guardada en un sobre que se cierra con cinta de seguridad, firmado de manera manuscrita por el auditor, el contralor interno del IECM y el secretario ejecutivo del IECM. Finalmente, se resguarda en la caja fuerte de la oficina del secretario ejecutivo del IECM.

La computadora utilizada para la configuración, así como el servidor de administración de la elección, no tienen conexión a internet. La computadora se conecta al servidor, a través de un enlace ethernet, a fin de realizar la configuración de la elección. Todo ello previene que existan atacantes externos que intervengan la comunicación entre la computadora y el servidor.

> El sistema de configuración solamente es accesible por el administrador del sistema, quien tiene que ingresar cuatro contraseñas alfanuméricas.[166]

El informe señala algunos riesgos sobre esta etapa. Uno de los más importantes es que "no se realizó [...] una auditoría y la consiguiente firma del código correspondiente al módulo de registro de votantes" para esta elección, por lo que una **parte del *software* quedó sin auditarse por completo,** quedando sin firmar y resguardar también. También aquí es fundamental ser claros: si un atacante o algún funcionario corrompido manipulara ese código para alterar la elección, sería suficiente para tomar el control de la misma.

Otro punto fundamental es que parte del SEI **funciona con *software* de terceros:** algunas "funciones clave para dotar de seguridad a los procesos" son hechos con programas (*Quickhash* y *SeguriDoc*) que **no son auditados** (lo que afecta la generación de claves y la firma digital). Cuando analizamos los casos de VPI en EUA, vimos varios ejemplos que muestran los riesgos y las pésimas prácticas en seguridad que tienen las empresas (y lo fácil que es aprovecharse de ello para vulnerar un sistema), por lo que este hecho también debería ser preocupante para la legitimidad de la elección como un todo.

Por si esto no fuera poco, la computadora donde se realizó la firma del código, primero, no fue auditada previamente (ni custodiada), por lo que es posible, al menos hipotéticamente, que contuviera algún *malware* que afectara la elección (y tampoco se verificó que la clave de la elección no quedara grabada una vez que se capturaba, tal como pueden hacer algunos programas maliciosos, tales como *keylogger*) y, segundo, era una computadora de uso regular en el Instituto e incluso contenía otros programas ajenos a la tarea de firma, cifrado y configuración, lo que aumenta considerablemente los riesgos de seguridad.[167] El descuido en este punto es gravísimo, porque utilizar dispositivos no auditados que puedan ser infectados en el uso común facilita mucho tomar el control del sistema.[168]

Aquí es muy importante recordar que en todos estos casos, si la elección se hubiera comprometido al infectar el sistema de alguna forma,

166. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, pp. 5-6.
167. *Ibidem,* p. 6.
168. No sólo pensando en casos de uso de *malware* dirigido a la computadora sino de casos tan simples como la infección dentro de las prácticas de *botnets* con las que después puedan infectar un programa para manipular el *software.*

no habría forma de saberlo porque el diseño de los sistemas de VPI hace que una vez que se tomó control de ellos el atacante pueda borrar todos los rastros, haciendo imposible saber si un fraude se realizó. Incluso en el caso de la revisión del "Avance de la votación", que suele usarse como un filtro para saber que el sistema está íntegro, es perfectamente posible (y de hecho una práctica común en *hackeos* de este tipo) configurar el *malware* para decir que el sistema está cerrado aunque no lo esté, para luego manipular votos y alterar la elección a discreción.

El informe además señala fallas de la normativa por su vaguedad sobre los procesos de seguridad. Por ejemplo, el resguardo de la llave de apertura del sistema no tiene detalles tales como el timbrado, el lugar donde se deposita la llave y los mecanismos de custodia y los dispositivos que se usan para su generación (los *Lineamientos* sólo señalan que la llave "será resguardada conforme a los procedimientos y mecanismos que para tal efecto se determinen", en su artículo 24).[169] Como es de imaginarse, esta situación implica, por un lado, riesgos internos para el sistema mismo y, por otro lado, el incumplimiento del requisito de certeza en cuanto al principio de legalidad (que las disposiciones relacionadas con la reglamentación del derecho estén en una ley de forma clara y precisa).

En cuanto al **proceso extendido de votación por Internet** (del 8 al 12 de marzo). Los controles de seguridad fueron los siguientes:

> El proceso de autenticación requiere que, al momento de utilizar la aplicación, el votante cuente con tres elementos: credencial de elector, contraseña y teléfono, cuyo número registró previamente y en el que se recibe el token. La combinación de estos elementos conlleva que la autenticación sea robusta, evitando ataques de usurpación por parte de personas no cercanas al votante.
>
> La sesión de votación caduca en 15 minutos, lo que impide en buena medida ataques de suplantación de identidad causados, por ejemplo, por extravíos del teléfono.
>
> El voto se firma digitalmente, luego se cifra y es enviado a través de SSL. La firma y el cifrado se realiza con RSA. Finalmente, el voto se vuelve a cifrar con una función del manejador de base de datos Oracle. Asumiendo una correcta implantación del cifrado, el proceso descrito asegura tanto la confidencialidad del voto como su integridad.
>
> Los votos se almacenan en un servidor ubicado físicamente en las instalaciones del IECM. El centro de datos en donde se encuentra el servidor cuenta con medidas

169. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, p. 6.

> de control de acceso, de manera que es difícil que una persona no autorizada ingrese al lugar sin advertirlo.
>
> Los votos se almacenan de manera aleatoria en una de las 7 tablas o "urnas virtuales" disponibles en la base de datos, a fin de confundir el orden en que se recibieron los votos y de esta manera romper la relación voto-votante.
>
> Tanto la información de la cantidad de votos recibidos como el estatus del sistema se observan desde el módulo de administración, a donde accede el administrador del sistema.[170]

En primer lugar, sabemos que el robo de credenciales de los usuarios puede realizarse antes de que emitan su voto y entre en el proceso de cifrado. Pero además de este riesgo general de los usuarios está el hecho de que el voto remoto habilita la manipulación del voto de una persona porque carece de un entorno seguro para votar. Una persona viviendo en el mismo domicilio puede acceder a los elementos de autenticación o usar el dispositivo de otra persona una vez que se autenticó. En segundo lugar, está el hecho de que el servidor donde se almacena todo el SEI está en las instalaciones del IECM, por lo que no se cuenta con un sistema de redundancia de datos en otro servidor. Un tercer problema directamente relacionado con la secrecía y la integridad del voto es señalado claramente en el informe:

> Si bien los votos se almacenan de manera aleatoria en diferentes tablas a fin de romper la relación voto-votante, existe aún la posibilidad de que se pueda deducir dicha relación, especialmente teniendo privilegios de acceso al sistema y/o base de datos. Elementos como la hora en que se guardan, además de *logs* de sistema o *logs* del tráfico de red entrante pueden utilizarse para encontrar la relación.[171]

Lo que el párrafo anterior quiere decir es que la posibilidad de des-anonimizar los votos es real (y bastante simple teniendo el acceso a cierta información). Una falla así es grave y ni siquiera se trata de un problema relativo a los riesgos externos del sistema (un *hackeo* específico que vulnere los mecanismos de anonimización, tal como explicamos más arriba). La razón de este riesgo puede ser o bien un desconocimiento o un descuido general sobre cuestiones mínimas de seguridad, tal como sucede también con el hecho de que al momento de cerrar el sistema (al final de la jornada ampliada el 12 de marzo) la dirección de acceso al servidor fue visible (tanto la de la versión de intranet como la de Internet), lo que facilita la posibilidad

170. *Ibidem,* p. 8.
171. *Ibidem,* p. 8.

de realizar distintos tipos de ataques como pueden ser los de denegación de servicio.[172]

Al momento de abrir la urna virtual para realizar el cómputo de votos el peso de la seguridad recae sobre la clave privada de la elección que está en la memoria USB que tiene el Secretario Ejecutivo del IECM (necesaria para abrir las urnas virtuales, junto con la contraseña que también tiene el Secretario). La USB está en riesgo y con ella la elección como un todo, porque si se daña o pierde, es imposible descifrar los votos.[173] Aquí es importante señalar que los votos se almacenan varios días antes de ser contabilizados el 13 de marzo, con lo que se abre una ventana de tiempo considerable en la que se pueden realizar ataques a la elección. Además, una vez contados estos votos, la información queda "congelada" hasta el 15 de marzo, cuando se celebra la jornada electoral complementaria, lo que deja un espacio para que la información de la votación por Internet se filtre, afectando la elección.[174]

El 15 de marzo, el SEI se configura nuevamente para la jornada complementaria. Un primer problema aquí, es que los archivos de los catálogos que se cargan al sistema (lista nominal, candidaturas, proyectos, etc.) son validados sin transparencia ni auditabilidad por la unidad correspondiente; es decir, que **"no se puede tener certeza de que dichos archivos se mantienen íntegros hasta su carga en el sistema"**, lo que implica que su integridad no está demostrada. Por eso una recomendación del informe fue que se firmen digitalmente para verificarlos antes de cargarlos en el sistema. El problema es grave porque se podría manipular la lista nominal para negar el derecho al voto o modificar los proyectos que se presentan para ser votados.

Otro problema es que la jornada del 15 de marzo usa la misma llave criptográfica que la de la jornada ampliada del 8 al 12 de marzo, lo que es peligroso porque facilita ataques que utilicen *malware* para tomar control del sistema y da un tiempo mayor donde puede existir una manipulación deliberada. El riesgo se señala en el mismo informe al decir que en estos casos: "La integridad de la jornada del día 15 de marzo estaría, por lo tanto, en entredicho".

172. *Ibidem*, p. 8.
173. *Ibidem*, p. 9.
174. *Idem*.

¿Qué sucedió en la práctica en la votación por Internet? Las autoridades implementaron un formato único de voto por Internet para tres distritos electorales (9, 12 y 13) y para parte del distrito 5, en los que instalaron módulos con iPad's con la *App* para votar. Cada módulo contaba con un funcionario que tenía un código QR y un número de identificación personal (NIP) para operar el *iPad*. La modalidad única implicaba que, en caso de que el sistema fallara, las personas no podrían ejercer su derecho a votar, tal como sucedió ese día.[175]

Cuando la jornada termina, el cómputo de votos se hace cargando la llave criptográfica que tiene el Secretario Ejecutivo, por lo que si él no está es, al menos teóricamente, imposible descifrar los votos de manera oficial. Más grave aún es el hecho de que la llave se carga cuando la elección aún está abierta, lo que significa que el sistema está conectado a Internet y eso "presenta el riesgo de que pueda lograrse acceso indebido a la llave, bien a través de Internet bien directamente del servidor por personal del IECM. Podrían entonces descifrarse votos anticipadamente, tanto los que ya están almacenados en la base de datos como los que están llegando, siendo este último caso más peligroso **ya que se pueden descifrar y ligarlos a la identidad del votante**" [Énfasis nuestro]. No sólo el sistema puede ser comprometido para tomar control de él, sino que la secrecía del voto se pone en juego por completo.[176]

El informe señala que las auditorías realizadas por el IECM no son suficientemente profundas en cuanto a algunos elementos fundamentales de los riesgos de votar por Internet:

> Si bien en el seno del IECM, así como por parte de la entidad auditora, se han realizado análisis de riesgos del sistema de elección por internet, en estos se ha contemplado primordialmente la infraestructura de servidores y comunicaciones, con un enfoque del flujo, operación y continuidad del sistema. En cambio, **dichos análisis han profundizado poco en otros elementos fundamentales del sistema electrónico por internet, como el propio *software*, la información sensible y los diversos procesos que sustentan una elección, todo ello orientado a la protección de los principios democráticos y sus consecuentes requisitos de seguridad en un entorno de voto electrónico. Tampoco quedan de manifiesto en dichos análisis los diversos tipos de atacantes y las motivaciones que pudieran tener para atentar contra la integridad de la elección.** Estos aspectos

175. *Ibidem,* p. 11. En la reunión donde R3D participó, el 20 de enero del 2020, ésta fue una de las objeciones que presentamos y uno de los riesgos que advertimos. Las autoridades nos respondieron que "el sistema era seguro y contaban con medidas para corregir eventuales problemas".
176. *Ibidem,* p. 12.

son importantes ya que permiten estimar de una manera más aproximada los posibles riesgos, la probabilidad de ocurrencia y el impacto que tendría cada uno en caso de suceder.

En este sentido, se recomienda realizar un proceso exhaustivo de estimación de riesgos del voto por internet, en donde se considere que hay atacantes que buscarán realizar infiltraciones, manipulaciones o atentar en contra de la integridad de la elección. **Dicho análisis de riesgos debe considerar todos los tipos de atacantes, entre los que se pueden incluir votantes, criminales informáticos, partidos políticos, personal del IECM, responsables de mesas electorales o gobiernos extranjeros**, entre otros. Al realizar una estimación de riesgos amplia y profunda se podrá determinar, con mayor precisión, los mecanismos técnicos, políticos y procedimentales que deben implantarse para contar con un sistema y un entorno seguro de voto por Internet.[177]

Una afirmación como ésta deja claro que el enfoque adoptado por el IECM sobre la seguridad del sistema de voto por Internet es inadecuado y que, por desconocimiento o desinterés, los riesgos principales no han sido evaluados como deben serlo. El análisis superficial de la seguridad de un sistema de voto por Internet es muy grave y pone en entredicho todo lo que se ha señalado sobre la seguridad y la garantía de los principios del voto y los principios rectores de las elecciones. ¿Cómo podemos sostener que el voto por Internet es seguro en México si su seguridad ni siquiera ha sido evaluada como debe ser? El problema parece ser más grave de lo que creíamos al principio porque no sólo se trata de que la revisión del sistema sea poco transparente y cerrada (la experiencia comparada nos muestra que los sistemas de VPI suelen ser así), sino que hoy podemos saber que esa caja negra (cuyo interior no podemos ver) no está haciendo lo que nos dicen que hace.[178]

Además de las claras insuficiencias en seguridad, el sistema también tiene fallas importantes en materia de transparencia. Este punto ilustra muy bien la **tensión entre la secrecía del voto y la integridad del sistema y las elecciones** que desarrollamos más arriba como uno de los puntos centrales para analizar en el caso del VPI.

177. *Ibidem,* pp. 14-15.

178. Si la seguridad ha sido evaluada en el mejor de los casos de forma incompleta, decir que el voto por Internet es seguro no tiene fundamentos. Sin embargo, el IECM presenta el informe externo como un logro en el que el VPI se mantiene de manera íntegra, tal como lo expresó el Consejero Electoral Yuri Beltrán Miranda en la Quinta Sesión Ordinaria del 28 de mayo del 2020. Disponible en: https://www.youtube.com/watch?v=yxjK57N5-U0&feature=youtu.be, a partir del minuto 33.

> La verificación individual es un aspecto muy importante para validar el correcto funcionamiento de un sistema de voto electrónico **ya que permite combatir la opacidad inherente a esta tecnología. Su principal objetivo consiste en que el votante pueda estar seguro que su voto se ha registrado correctamente.** En sistemas convencionales basados en papel, los ciudadanos pueden verificar que su voto es recibido correctamente ya que son ellos mismos quienes colocan la boleta en la urna física y, sea personalmente como observadores o indirectamente a través de los interventores de partidos políticos, puede garantizarse que la urna permanece cerrada hasta el escrutinio y no se alterna su contenido mediante la sustracción de boletas o la adición de votos indebidos.
>
> **En el voto electrónico, por el contrario, un mensaje de mera confirmación de que un voto ha quedado correctamente registrado no proporciona garantía ni de que el voto realmente se haya transmitido conforme a la intención del elector ni de que se haya además almacenado tal y como fue emitido. En este sentido, el programa de voto electrónico puede estar diseñado para ofrecer un mensaje tranquilizador al elector mientras se altera subrepticiamente el contenido de su sufragio.** Adviértase además que la posibilidad de que un voto no se registre adecuadamente no se asocia directamente con una falla o manipulación del *software*. **En entornos de votación remota, en donde los dispositivos desde los que se emite el voto no están bajo el control y supervisión de la autoridad electoral, es posible que exista *malware* en el dispositivo del cliente que manipule la intención del voto antes de que este sea cifrado y transmitido.**[179]

Como sabemos, los problemas de la oscuridad del VPI nos llevan de vuelta siempre a los problemas de seguridad y manipulación del sistema.[180] Ya que para fortalecer la secrecía del voto estos sistemas no entregan ningún comprobante en el sentido descrito en estos párrafos, si la intención del voto es manipulada no es posible darnos cuenta de que el fraude tuvo lugar.[181]

Además, el elemento de *verificación individual* está faltante por completo. Las y los electores reciben la confirmación de que su voto fue enviado y recibido, pero esto no es equivalente a tener una verificación

179. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, p. 15.
180. *Ibidem,* p. 21. El propio informe reconoce esta realidad inherente al uso de la tecnología y la votación por Internet, al hablar de los registros que los sistemas generan tras cada acción que realizan y que, en principio, servirían para poder darnos cuenta si el sistema fue manipulado. El problema, obviamente, está en que: "Pese a las ventajas que ofrece la generación de *logs* a nivel de sistema o red, no se puede garantizar sólo con ellos un mecanismo certero para una auditoría post-electoral, ya que puede haber casos de atacantes con privilegios de acceso, por lo que también podrían modificar los *logs* a fin de eliminar cualquier prueba de la manipulación".
181. En la reunión celebrada con el IECM el 22 de enero de 2020, una de nuestras preguntas se relacionó específicamente con este punto, en donde cuestionamos sobre si existía algún registro o elemento de verificación sobre el sentido del voto. La respuesta del IECM fue que eso no era posible porque ponía en riesgo el secreto del voto.

individual como sucede en Estonia, por ejemplo. **La verificación personal es imposible** y este es un punto importante para evaluar la confiabilidad del sistema en general (porque no existe una garantía de que el mecanismo haga lo que dice que hace). El VPI queda en un callejón sin salida porque, en caso de generar mecanismos de verificabilidad individual (como enviar un comprobante con la intención del voto), el secreto y la libertad del voto se pone en riesgo (ante el hecho de que alguien pueda conocer sus preferencias políticas),[182] lo que a su vez implica riesgos relacionados con la coacción, la compra y la venta de votos, la persecución política y otros actos de represalia como puede ser el condicionamiento de apoyos sociales, particularmente problemático en países con una desigualdad profundizada como es México.

Obviamente, las limitaciones de la verificabilidad individual afectan la verificabilidad universal que el sistema debería tener (lo que se conoce como *End-to-End Verifiability*) y que consiste en saber que todos los votos fueron hechos y almacenados de acuerdo a la voluntad de las y los electores. Si prestamos atención podemos ver que esto afecta críticamente los principios de máxima publicidad y la posibilidad del control ciudadano, porque el grado de complejidad que implica la criptografía –indispensable para garantizar y explicar la verificabilidad universal– generalmente requiere de conocimiento especializado que sólo tiene la comunidad técnica. Al advertir este punto, el informe señala que:

> La solución [para el problema de la verificabilidad universal] propuesta en algunos países, como Noruega, Estonia o Suiza, consiste en articular esta última fase de tal forma que pueda ser verificada por cualquier actor interesado. **Debido a su complejidad criptográfica, tal etapa ya no está al alcance de cualquier ciudadano,** pero pueden preverse sistemas para que cualquier técnico pueda verificar por sí mismo si la apertura de la urna digital, el filtrado de los votos y el escrutinio se realizan de forma correcta. **Se trataría, en definitiva, de ofrecer un método de verificación neutro e independiente disponible para todo aquél con suficiente capacidad técnica. Todo ello contrasta con lo que sucede hoy en día en el escrutinio ya que se halla sometido únicamente al control de una entidad auditora contratada por el propio IECM.**[183] [Énfasis añadido]

¿Dónde quedan los principios de transparencia, máxima publicidad y control ciudadano cuando un paso fundamental de la elección puede ser evaluado sólo por una élite técnica? ¿Qué certeza existe de que las elecciones son lo que deberían ser cuando no podemos ver sus etapas ni entender cómo

182. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico*, 30 de abril de 2020, p. 16.
183. *Ibidem,* p. 17.

funciona el sistema por el que se desarrollan? ¿Cómo mantener la legitimidad de las elecciones si no es apelando, una vez más, al acto de fe de creer que el sistema funciona como nos dicen y sustituyendo el escrutinio público por la confianza ciega en las autoridades y -específicamente- en las tecnologías?

Todas estas preguntas, además, deberían responderse tomando en cuenta el contexto histórico, económico, político y social de México. Tal como el informe apunta (señalando en particular la Ciudad de México), el contexto electoral está marcado por el riesgo constante del clientelismo y de las muchas formas en que la coacción del voto puede tener lugar. Al mismo tiempo, el contexto del voto por Internet se suma a una dinámica electoral en la que sabemos que distintos sujetos intentan manipular la intención de las y los votantes.[184] El fantasma del fraude en México está presente de manera casi permanente y cada elección implica un serio reto para la legitimidad de las elecciones y de las instituciones relacionadas con asegurar la democracia. Es en este contexto que las respuestas a estas preguntas dejan un silencio que es más bien desolador.

Finalmente, el informe hace un análisis de las auditorías realizadas para evaluar el sistema de VPI. A partir de esta revisión podemos señalar seis puntos que no sólo confirman sino que refuerzan las preocupaciones y peligros que hemos advertido a lo largo de este trabajo.

→ Primero. En cuanto al principio de transparencia, si bien reconocen que las auditorías son un elemento importante para la evaluación técnica, señalan que esto debe tomarse sólo como **un primer paso que está relacionado con la confianza de la ciudadanía:**

> "que debe ir acompañado de otros parámetros [...] por ejemplo, conocer cómo se ha seleccionado al auditor, de qué tiempo ha dispuesto para llevar a cabo el análisis técnico, qué información le ha sido proporcionada, cuáles han sido las cláusulas de confidencialidad pactadas, cuál es el alcance real del análisis y, sobre todo, qué régimen de publicidad se aplicará al informe final de la auditoría".
>
> **Es absurdo, por lo tanto, contentarse con el mero hecho de que exista una auditoría ya que tal iniciativa podría quedar seriamente sesgada si los parámetros enunciados en el párrafo anterior no satisfacen lo que se espera de estos estudios técnicos.** En este sentido, conviene recordar que el motivo por el que se contrata una auditoría en este campo difiere de las razones por las que análisis similares se llevan a cabo en otras áreas. Normalmente, muchas aplica-

184. *Ibidem,* pp. 18-19.

ciones técnicas necesitan ser auditadas, o certificadas u homologadas, antes de su puesta en marcha. Se trata de procedimientos de armonización y control de calidad ampliamente implantados en todo proceso productivo.

En el caso del voto electrónico, las auditorías persiguen también tal armonización y calidad contrastadas, pero incluyen asimismo otros objetivos, como la generación de confianza entre los ciudadanos. La auditoría deberá verificar que el sistema funciona, pero también hacerlo de tal forma que los ciudadanos queden convencidos que no ha habido ningún fraude. **Este segundo objetivo es más difícil de lograr dado que, teniendo en cuenta la naturaleza propia del voto electrónico, los ciudadanos no tendrán otros elementos en qué apoyarse para comprobar la funcionalidad del nuevo instrumento. Mientras que cualquiera puede detectar si un tren alcanza o no la velocidad programada, el voto electrónico no ofrece tal facilidad para ser controlado y entonces la auditoría constituye un instrumento de gran ayuda, aunque su tenor literal será incomprensible para la mayoría de ciudadanos.** Se trata de un gesto de transparencia que, si bien no será comprensible para todos, sí podrá ser evaluado por expertos independientes e inyectar de este modo confianza suficiente en el conjunto de la ciudadanía.[185] [Énfasis añadido]

El principio de transparencia y el de máxima publicidad en clave de control ciudadano están en tensión inevitable e irresoluble con el voto por Internet. ¿Cómo es posible que estos principios se garanticen con un sistema que es prácticamente incomprensible "para la mayoría de los ciudadanos"? Si bien la preocupación de los investigadores del informe se concentra en cuestionar las limitaciones de las auditorías, que compartimos como correctas y que señalamos en el apartado correspondiente a las mismas, esta observación sirve para dar luz al problema más profundo de la naturaleza del sistema y de los problemas de comprensión general de la ciudadanía sobre su funcionamiento (y sus problemas subsecuentes para generar confianza y legitimidad política).

→ **Segundo.** A la par de la tensión con la transparencia y la publicidad, es claro que las auditorías no tuvieron ni el tiempo ni la profundidad suficientes para revisar el SEI de forma completa.[186] La falta de tiempo y las limitaciones a la profundidad de las auditorías son resultado de los ritmos y cambios normativos anticipados de las autoridades electorales (tan sólo cuatro meses antes de las elecciones con cambios relevantes para el sistema de votación), de la práctica cotidiana de las mismas (dado que sabemos que las auditorías de los años y ejercicios anteriores también

185. *Ibidem*, p. 22.
186. *Ibidem,* p. 23.

tuvieron estas dificultades), pero al parecer también de una concepción de fondo sobre lo que las auditorías deberían revisar (especialmente en materia de seguridad). El informe es claro en que el enfoque de las auditorías es sobre la funcionalidad más que sobre algunos niveles fundamentales de los riesgos del VPI en general. Por eso las pruebas de penetración y recompensa y la permisión de ingeniería inversa, que son fundamentales y se mantienen ausentes, son tan necesarias.

Tercero. Justamente en ese sentido, sea por cuestiones metodológicas o por razones de confidencialidad, remuneración, alcance del estudio, etc., la revisión del SEI ha sido siempre incompleta, sin posibilidad de analizar el código fuente ni otros componentes esenciales del sistema de forma independiente; es decir, que no es posible estudiar a profundidad el sistema de VPI de forma libre y completa, tal como se hizo en otros países donde se encontraron numerosas limitaciones a este tipo de sistemas. El informe subraya la hermeticidad del IECM y recomienda una mayor apertura. Citamos en extenso este punto porque no deja dudas de lo que aquí señalamos:

> Cabe añadir a todo ello que, a nivel estrictamente técnico, las preocupaciones por la seguridad del sistema son habitualmente rebatidas por gran parte de la comunidad académica al entender que la oscuridad nunca es la mejor forma de alcanzar la mayor seguridad en una aplicación informática. *Security by obscurity* no es, en este sentido, un patrón de comportamiento recomendable y el IECM es consciente de ello ya que por eso se admite la participación de una firma auditora, **aunque se hace de forma limitada y con un aperturismo menos ambicioso del hallado en otros países.**
>
> En relación con los criterios utilizados para seleccionar a la entidad auditora, cabe señalar que **los datos disponibles son por el momento escasos.** Partimos de lo señalado en los propios Lineamientos al prever "una auditoría pública en cada una de sus etapas de desarrollo e implementación, a través de instituciones o empresas con prestigio internacional" (art. 48). A tenor de esta formulación, cabe indicar, en primer lugar, que **no se excluye la posibilidad de que entidades de lucro participen en la auditoría pública.** Se emplea, por otro lado, una formulación difusa y genérica como la de "prestigio internacional", que, salvo que se concrete en algún otro tipo de disposición, pierde casi toda eficacia real. Quedan excluidos entes de dimensión únicamente local, pero el abanico de otras Instituciones susceptibles de encajar en esa definición de prestigio internacional es demasiado amplio. Sería recomendable, en este sentido, que el IECM estableciera criterios más rigurosos para poder acotar el perfil de entidades susceptibles de llevar a cabo la auditoría.
>
> [...]

En el caso de estudio, la Facultad de Estudios Superiores (FES) Aragón de la UNAM ha llevado a cabo la auditoría. Se trata de la misma entidad que ha venido colaborando con el IECM en los últimos años y que, entre otras tareas, también desarrolló la auditoría externa encargada en julio de 2017 con la perspectiva de uso del voto electrónico en las elecciones de 2018. En aquella ocasión, otra entidad –Scanda Kimat– también llevó a cabo una segunda auditoría.

A tenor de los datos recabados del propio IECM, **no se realizó licitación pública para la auditoría, sino que se remitieron invitaciones directas a siete instituciones académicas con representación en la Ciudad de México.** Las invitaciones se cursaron a principios de febrero otorgando un plazo breve de tiempo para la respuesta de los potenciales interesados. **Se trata de una restricción temporal que daña la credibilidad del proceso ya que, más allá de sus causas reales, quizás justificadas por el calendario ajustado al que ya se ha hecho mención, puede ser percibida como una maniobra para excluir determinados candidatos.**

[...]

Por otro lado, debe señalarse que **la retribución es sufragada por el propio IECM,** lo que resulta congruente con el hecho de contar con una plataforma de voto electrónico desarrollada internamente en el Instituto. Se trata de un esquema diferente al existente en otros países en los que, al existir empresas con soluciones privadas de voto electrónico, las auditorías requeridas por la administración son financiadas por las propias empresas. Tal solución no es factible en el caso del IECM, pero **no debe olvidarse que identificar quién financia la auditoría constituye también un factor primordial para valorar la confiabilidad del producto resultante** y todo ello sin perjuicio de la calidad intrínseca que puedan tener los informes aportados, extremo que escapa al análisis que se lleva a cabo en este apartado.

Para terminar con el análisis del procedimiento de selección de una firma auditora, conviene hacer referencia a la existencia de acuerdos de confidencialidad entre la auditora y la entidad propietaria del producto. Tales documentos o Non-Disclosure Agreements (NDA) son de suma importancia ya que pueden contener cláusulas que comprometan la fiabilidad de todo el análisis. Puede suceder, por ejemplo, que ambas partes acuerden excluir ciertos aspectos de la auditoría o que acuerden llevarla a cabo sin consultar determinada documentación. Ambos pactos pueden ser razonables, pero, al estar incluidos en un acuerdo de confidencialidad, **los lectores desconocerán que están consultando un análisis realmente incompleto y ninguna de las partes podrá informarles al respecto ya que estarán ligadas al NDA que hayan suscrito.** Es por todo ello que los acuerdos de confidencialidad son de vital importancia. No olvidemos además que son moneda de uso corriente en las labores de auditoría.

En el caso que nos ocupa, el marco normativo establecido por el IECM no alude a ningún acuerdo de este tipo. Como ya se ha señalado, los Lineamientos prevén un instrumento jurídico acordado entre IECM y la entidad auditora en el que se detallarán las labores a realizar y la documentación a recibir, pero no se incluye ninguna mención a la confidencialidad. **Si se consulta el mencionado acuerdo,**

> **cuya publicidad no viene impuesta en los Lineamientos, interesa destacar la décima cláusula en la que, tras aludir a las obligaciones de confidencialidad de ambas partes y a la sumisión al ordenamiento jurídico, también se prevé la firma "de un acuerdo de confidencialidad o de No divulgación" entre la UNAM y el IECM.** Se trata, por lo tanto, de un nuevo acuerdo diferente al contrato en el que se incluye esta décima cláusula.
>
> Este documento no ha sido consultado para la realización de este informe y resulta imposible, por lo tanto, aventurar su contenido. Sea como sea, conviene alertar sobre su importancia en los casos de voto electrónico. Ya se ha mencionado que tales NDA son habituales en este tipo de tareas y su presencia no debería causar extrañeza, pero tampoco debe olvidarse que la finalidad de las auditorías de voto electrónico va más allá de la comprobación técnica y persigue afianzar la confianza ciudadana. **En este sentido, cualquier pieza que escape al control ciudadano es susceptible de crear dudas que empañen el conjunto del proceso. Es por ello que conviene evaluar la necesidad de contar con un acuerdo de este tipo y suprimirlo en caso de que no sea estrictamente preciso.**[187] [Énfasis añadidos]

Las conclusiones que podemos desprender del contenido del informe son preocupantes: i) el acuerdo que determina la confidencialidad y el alcance de la auditoría no es público (el Anexo técnico que sólo se entrega al IECM no es revisable por el público); ii) hay elementos de fondo esenciales para evaluar la seguridad y la integridad del sistema a los cuáles no se tiene acceso; iii) la apertura y publicidad del sistema está por debajo de lo que se acostumbra en otros países que implementaron el VPI y tuvieron buenas prácticas; iv) la selección de los auditores estos años no fue abierta ni existió una licitación pública, sino que se hizo por invitación y con poco tiempo para aceptar y participar; v) el IECM es quien paga estas auditorías, quien establece las reglas de su alcance y quien se queda con la información que no es hecha pública de esas auditorías, y; vi) en este caso los acuerdos de confidencialidad y la información reservada existen y dejan fuera de análisis información que es considerada vital para este tipo de estudios y está relacionada tanto con la seguridad y la integridad del sistema como con los principios centrales del voto y de las elecciones.

Esto significa que el sistema no sólo es opaco y cerrado en términos de su práctica pública (lo que se nos ha permitido ver y el discurso del IECM sobre la publicidad de las auditorías), sino que el funcionamiento de las auditorías es estructuralmente oscuro. Los principios de confidencialidad y no divulgación son incompatibles con la transparencia y la máxima pu-

187. *Ibidem,* pp. 25-28.

blicidad y confirman las dudas que adelantamos más arriba al analizar las auditorías sobre los documentos que se entregaban únicamente al IECM. Como sugiere el informe, prudentemente desde luego, las limitaciones de las auditorías y su hermetismo ponen en seria duda su credibilidad, si no la descartan por completo.

→ Cuarto. El informe también advierte que la etapa del registro de votantes no fue incluida en la auditoría del código fuente en el caso de las aplicaciones móviles como una falla importante; que las dos computadoras utilizadas para echar a andar el sistema tampoco fueron revisadas para saber si no contenían algún *malware* que pudiera afectar la seguridad de la elección y del sistema; y que no hay pruebas de que se realizara el análisis de los protocolos criptográficos utilizados más allá del nivel de infraestructura de redes, en particular en cuanto a sus niveles conceptual y de ejecución.[188]

Pero este no es el único caso en el que se realizan acciones incompletas o que no significan mucho en términos de seguridad. Como mencionamos más arriba, las declaraciones de apertura del sistema y del conteo de votos en cero significan poco y nada en estas condiciones porque si el sistema fue manipulado los observadores electorales no podrían darse cuenta del fraude de cualquier forma:

> Se trata de una medida positiva, pero, como en tantos otros casos relativos al voto electrónico, la mera presencia de observadores puede carecer de sentido si lo que se contempla, dada su complejidad técnica, realmente no puede verificarse.
>
> Es lo que sucede, por ejemplo, cuando se alude a inicialización en cero del sistema o a otros aspectos técnicos similares (art. 26 / Lineamientos). Celebrar una sesión solemne en la que se emitan certificados de este tipo no supone valor añadido alguno a los mecanismos de seguridad ya que tanto la pantalla en la que se observa el contador a cero como los certificados en papel pueden no corresponder a lo que realmente está sucediendo a nivel técnico en el seno de las computadoras. [189] [Énfasis añadido]

→Quinto. La investigación señala un cuestionamiento importante sobre dos de los argumentos a favor del VPI que refutamos en la Parte I de este trabajo: la usabilidad y comodidad de estos sistemas y el aumento de la participación política. En el primer caso, el informe reconoce que:

> Se trata de un mecanismo sofisticado que comporta el uso, entre otros elementos, de herramientas de reconocimiento facial juntamente con la necesidad de procesar la imagen y datos de la credencial de elector. Si todo ello acaba con un

188. *Ibidem,* p. 29.
189. *Ibidem,* p. 35

> resultado positivo, el elector recibirá los códigos y contraseñas correspondientes. **No se trata, por lo tanto, de un proceso fácil y, si incluso un usuario avezado en estas lides puede hallar trabas importantes, huelga señalar que sectores importantes de la población se revelarán incapaces de culminar con éxito todas las etapas.**
>
> El número de usuarios actuales se antoja bajo para poder extraer conclusiones definitivas al respecto ya que la cifra, a la vista del censo total, representa un porcentaje escaso, pero **cabe advertir, como dato quizás más revelador, de los bajos registros de votantes reales entre aquellos que ya habían procedido a todo el proceso de pre-registro y estaban ya autorizados a emitir su sufragio de voto remoto. Se contabilizaron un total de "3,159 votos y opiniones ..., lo cual corresponde al 31.52% de participación respecto del total de ciudadanas y ciudadanos que obtuvieron la clave de votación y opinión"**[190] (: 22 / Informe III). [Énfasis añadido]

Aunque ya habíamos mostrado que no existe causalidad entre el voto por Internet y el aumento de la participación, ni que el hecho de usar un sistema así hace que las personas lo elijan, la experiencia de años del VPI en la CDMX (que parece confirmarse en este último ejercicio) muestra que ninguno de los dos argumentos se sostiene (ni la participación aumenta de forma significativa ni el sistema resulta de fácil uso y elección). Las exigencias de seguridad llevan a tener un sistema demasiado complejo que exige cierta capacitación de uso (o, en otras palabras, cierto grado de educación digital o *expertise* de uso) que mucha gente no tiene ni desea (consciente o inconscientemente) tener. La optimización del sistema juega, por así decirlo, en contra sus supuestas ventajas. El ejemplo del porcentaje de personas que se identificaron para poder ejercer su derecho al voto por Internet y al final no lo hicieron no podría ser más ejemplificativo: sólo una de cada tres personas que realizaron el primer paso del procedimiento lo completaron al final.

Lisa y llanamente, y esto es algo mencionado por el informe,[191] los resultados de (al menos) la etapa actual del VPI en la CDMX contradicen el

190. *Ibidem,* p. 30.

191. Un señalamiento importante del informe en este sentido, que toma en cuenta la variable de la desigualdad y la brecha digital es el siguiente: "afirmar que todos los ciudadanos tienen fácil acceso a una computadora con conexión a Internet puede hacernos olvidar que el analfabetismo digital, sea total o funcional, sigue presente en determinadas capas de la población, que pueden tener además dificultades económicas para acceder a estos canales. Finalmente, el uso intuitivo que se atribuye al mecanismo de votación por Internet contrasta con el hecho de que, durante la jornada del día 15 de marzo, siguió existiendo un grado elevado de asistencia a los votantes". Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, p. 30. También se observó que hubo contradicciones en la forma de asistir a la gente en los módulos de votación presencial, resultando en inconvenientes y confusiones para los votantes, en parte derivadas por contradicciones o empalmes en las disposiciones aplicables (ver páginas 32 y 33 del informe).

estudio de viabilidad que sostiene que el SEI es de uso "fácil y dinámico", y también los dichos del Comité Técnico acerca de que el sistema era "intuitivo". En este punto es claro que varios de los supuestos beneficios que han sido señalados sistemáticamente para impulsar el VPI en los últimos años no se corresponden con la realidad.

→ **Sexto.** Al final de todo, el sistema falló. Varios de los distritos donde el VPI se habilitó como mecanismo único para votar tuvieron que cambiar a boletas tradicionales de papel después de varias horas de espera en las que el SEI no funcionó (las cuales demoraron más de dos horas en algunos casos), teniendo como resultado que muchas personas desistieran de participar y perdieran su derecho al voto. Aunque no existe información completa sobre las causas, está documentado que en algunas casillas el sistema falló y no pudo ser reactivado.[192] En el caso de la jornada del 15 de marzo, por ejemplo, un error en el uso de las tabletas iPad y la conectividad hizo que muchas personas no pudieran votar: "Este error tuvo como consecuencia directa la privación del ejercicio del voto para muchos ciudadanos".[193]

La conclusión de la última auditoría de la UNAM que señalaba que el sistema era suficientemente fuerte para resistir situaciones de ataques de denegación de servicio se "reveló falsa durante la jornada de votación", ya que en dos de los distritos el sistema simplemente no pudo rehabilitarse. Esto no significa que la auditoría fuera malintencionada o mentirosa, sino que esto es parte de las fallas comunes que son casi imposibles de advertirse (en especial con auditorías limitadas) en los sistemas de VPI.[194]

En el ánimo de hacer que las jornadas electorales funcionaran, la autoridad electoral cometió el error (muy probablemente con las mejores intenciones de llevar a buen puerto el ejercicio electoral) de generar un riesgo enorme para la seguridad del sistema mismo. En la jornada ampliada del 8 al 12 de marzo, la plataforma falló para los dispositivos Android, impidiendo que algunas personas ejercieran su voto. ¿Cómo se reparó el

192. *Ibidem*, p. 30.
193. *Ibidem,* p. 37.
194. *Ibidem,* p. 37-38. Relacionado con estas irregularidades está el hecho de que los reportes en algunos de los distritos en los que hubo irregularidades solamente señalan que "hubo errores que no pudieron subsanarse", como sucedió en los distritos 9 y 12.

problema? "realizando unos ajustes en el código" por un técnico facultado para ello. ¿Pero qué implica hacer una modificación del código fuente de un sistema de VPI? Implica "que se modifica un código que había sido previamente cifrado y sellado para así evitar manipulaciones posteriores". La modificación del código no estuvo acompañada por la repetición de una auditoría para asegurar su integridad y no hay nada en los informes que señale que se realizara un nuevo cifrado. Si recordamos la Parte II de este trabajo, en particular a partir de la experiencia de Estonia, sabemos que esta irregularidad es ideal para comprometer por completo la seguridad del sistema y de las elecciones.[195]

IV. Conclusión

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

195. Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico,* 30 de abril de 2020, p. 30.

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 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.

Bibliografía e informes especializados sobre voto por Internet

ANCIM. "Securing the Vote. Protecting American Democracy", September 2018. Disponible en: https://www.nationalacademies.org/news/2018/09/securing-the-vote-new-report.

Archer, Keith, *et. al. Recommendations Report to the Legislative Assembly of British Columbia*, Independent Panel on Internet Voting, February 2014, p. 12.

Bochsler, Daniel. Can Internet voting increase political Participation? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections. In: Paper Prepared for Presentation at the 'Internet and Voting' Conference. Fiesola, June, 2010.

Cardillo, Anthony & Essex Aleksander. "The Threat of SSL/TLS Stripping to Online Voting", *Springer*, 2018, p. 39.

Dworkin, Ronald. *Taking Rights Seriously*, Cambridge, Massachusetts, Harvard University Press, 1978.

Moher, E., Clark, J., Essex, A.: Diffusion of voter responsibility: potential failings in E2E voter receipt checking. USENIX J. Election Syst. Technol. (2015).

Culnane, Chris; Eldridge, Mark; Essex, Aleksander; Teague, Vanessa. *Trust Implications of DDoS Protection in Online Elections*, CSCR, 3 August 2017. Disponible en: https://arxiv.org/pdf/1708.00991.pdf.

FBI (Federal Bureau of Investigations), Agencia Ciberseguridad y Seguridad de Infraestructura (CISA por sus siglas en inglés), Departamento de Seguridad Nacional (*Department of Homeland Security*), Comisión de Asistencia Electoral y el Instituto Nacional de Estándares y Tecnologías. "Risk Management for Electronic Ballot Delivery, Marking, and Return", May, 2020.

Fitzgerald, Caitriona; Smith, Pamela; Goodman, Susannah. *The Secret Ballot at Risk: Recommendations for Protecting Democracy*, Electronic Privacy Information Center, Verified Voting and Common Cause, August 18, 2016.

Germann, Micha y Serdült, Uwe. "Internet voting and turnout: Evidence from Switzerland", *Electoral Studies,* Vol. 47, June 2017.

Goodman, Rachel y Halderman, Alex J. "Internet Voting is Happening Now. And it coul destroy our elections", 15 de enero de 2020. Disponible en Slate: https://slate.com/technology/2020/01/internet-voting-could-destroy-our-elections.html.

Habermas, Jürgen, *Entre naturalismo y religión*, España, Paidós, 2006, pp. 127-28.

Halderman, Alex J. *Hacking the D.C. Internet Voting Pilot*, Freedom to Tinker, June 2012. Disponible en: https://freedom-to-tinker.com/2010/10/05/hacking-dc-internet-voting-pilot/.

–. *Security Analysis of Estonia's Internet Voting System*, 31st Chaos Communication Congress (31C3), Hamburgo, Alemania. December 2014.

Halderman, J.A.; Teague, V.: The New South Wales iVote system: security failures and verification flaws in a live online election. In: Haenni, R., Koenig, R.E., Wikstrom, D. (eds.) VOTELID 2015. LNCS, vol. 9269, Springer, Cham, 2015.

Haynes, Peter. "Online Voting: Rewards and Risks", Intel Security, 2014.

Helger, Lipmaa. *Paper-voted (and why I did so)*, March 5 2011. Disponible en: https://helger.wordpress.com/2011/03/05/paper-voted-and-why-i-did-so/.

J. M. Porup. *Online voting is impossible to secure. So why are some governments using it?*, CSO, May 2 2018. Disponible en: https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html.

Jefferson, David. *If I Can Shop and Bank Online, Why Can't I Vote Online?*, Verified Voting, 2019. Disponible en: https://www.verifiedvoting.org/resources/internet-voting/vote-online/.

Krimmer, Robert; Duenas-Cid David; & Krivonosova, Iuliia. "New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper?", *Public Money & Management,* 2020.

Newman, Lily Hay. *Online Voting Has Worked So Far. That Doesn't Mean It's Safe*, WIRED, May 12 2020.

Norden, Lawrence. *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost,* The Brennan Center for Justice, New York University, 2006.

OSCE. *Estonia, Parliamentary Elections*, 6 March 2011: Final Report, 6 March 2011.

Rawls, John. Political Liberalism, New York: Columbia University Press, 1993.
—. *El derecho de gentes y "una revisión de la idea de la razón pública"*, Barcelona, Paidós, 2001.

R3D: Red en Defensa de los Derechos Digitales, *El Estado de la Vigilancia: Fuera de Control*, México, Noviembre de 2016.

Sartori, Giovanni. *¿Qué es la democracia?*, Bogotá, Altamir, 1994.

Sebes, E. John. *A hackes case for election technology,* OSET Institute, August 6 2013.

Simmons, Barbara. Report on the Estonian Internet Voting System, 3 de septiembre del 2011.

Specter, Michael; Koppel, James & Weitzner, Daniel. *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, The First Internet Voting Application Used in U.S. Federal Elections,* report from MIT researchers. Disponible en: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.

Springall, Drew; Finkenauer, Travis; Durumeric, Zakir; Kitcat, Jason; Hursti, Harri; MacAlpine, Margaret and J. Alex Halderman. Proceedings of the 21st ACM *Conference on Computer and Communications Security* (CCS '14), November 2014.

Trail of Bits. Full Report on the Voatz Mobile Voting Platform. March 13, 2020. Disponible en: https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/.

Trechsel, Alexander; Vassil, Kristjan. Internet Voting in Estonia: a Comparative Analysis of Four Elections since 2005, Report for the Council of Europe, 2010.

Valle Monroy, Bernardo. "México y el voto electrónico en ejercicios de participación ciudadana", Revista #DDA, 1 de abril de 2019.

Wells, Peter. *The cost of online voting,* Hackernoon (blog), November 11th 2017. Disponible en: https://hackernoon.com/the-cost-of-online-voting-dbca9e382c78.

Documentos del IEDF, IECM y del INE:

IECM. Acuerdo IECM/ACU-CG-014/2017.

IECM, *Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación,* Ciudad de México, 2017.

IECM. *Voto desde el extranjero bajo la modalidad electrónica. Experiencia, herramientas y condiciones técnicas, materiales y jurídicas para su implementación,* julio de 2017.

IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Jurídica Normativa,* julio de 2017.

IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Jurídica Normativa,* julio de 2017.

IECM. *Voto desde el extranjero bajo la modalidad electrónica - Implementación a través del Sistema de Voto Electrónico por Internet, perspectiva Operativa Procedimental,* julio de 2017.

IECM. *Estadística de Resultados. Elección de comités ciudadanos y consejos de los pueblos 2016. Consulta ciudadana sobre presupuesto participativo 2017,* Tomo II, 2017.

IECM. *Estadística de resultados de la Consulta ciudadana sobre presupuesto participativo 2018, IECM,* septiembre de 2018.
CGIEDF. Acuerdo ACU-69-11.

CGINE. *Lineamientos para el Desarrollo del Sistema del voto electrónico por Internet para mexicanos residentes en el extranjero,* INE/CG770/2016.

INE. *Reglamento de Elecciones,* 2016.

INE. Resolución LP-INE-003-2020 sobre la licitación para la auditoría sobre el voto por Internet

Documentos del IEDF, IECM y del INE:

Convención Americana sobre Derechos Humanos, 7 al 22 de noviembre de 1969, Organización de Estados Americanos.

Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948, Resolución 217 A(III), Asamblea General de las Naciones Unidas.

Pacto Internacional de Derechos Civiles y Políticos, 23 de marzo de 1976 (entrada en vigor), Resolución 2200 A (XXI), Asamblea General de las Naciones Unidas.

Notas periodísticas:

Excelsior. *Coronavirus impulsa el voto vía remota; INE probará sufragio por Internet en el 2021, Aurora Zepeda, 22 de mayo de 2020.* Disponible en: https://www.excelsior.com.mx/nacional/coronavirus-impulsa-el-voto-remota-ine-probara-sufragio-por-internet-en-2021/1383535.

Forbes. En 2018 hubo más de 4.3 millones de quejas por fraudes cibernéticos en México. 16 de mayo de 2019. Disponible en: https://www.forbes.com.mx/fraudes-ciberneticos-superan-las-4-3-millones-de-quejas-en-mexico/.

Herald Tribune. "Dutch government scraps plans to use voting computers in 35 cities including Amsterdam", The Associated Press, October 30, 2006. Disponible en: https://web.archive.org/web/20061119103008/http://www.iht.com/articles/ap/2006/10/30/europe/EU_GEN_Netherlands_Voting_Machines.php.

Hoja de Ruta. "Piden explicación sobre falla del sistema electrónico de votación por Internet en elección de Copaco y presupuesto participativo", 23 de marzo de 2020. Disponible en: https://hojaderutadigital.mx/piden-explicacion-sobre-falla-del-sistema-electronico-de-votacion-por-internet-en-eleccion-de-copaco-y-presupuesto-participativo/.

IDGNOW. Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil, 20 de novembro 2009. Disponible en: https://web.archive.org/web/20120601054809/http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/.

La Jornada. "Busca el IECM reponer votaciones en CDMX", 26 de marzo de 2020. Disponible en: https://www.jornada.com.mx/ultimas/capital/2020/03/26/busca-el-iecm-reponer-votaciones-en-cdmx-7759.html.

MIT News Office. *MIT researchers identify security vulnerabilities in voting app,* February 13, 2020. Disponible en: http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.

Noticias Electorales. "(México) Concluye INE Simulacro de voto electrónico por Internet con éxito", 30 de marzo de 2020. Disponible en: https://www.noticiaselectorales.com/mexico-concluye-ine-simulacro-de-voto-electronico-por-internet-con-exito/.

RTE. "Report raises e-voting equipment concerns", December 8, 2002. Disponible en: https://www.rte.ie/news/2002/1208/32905-voting.

SUM. "Fraudes financieros provocan pérdidas por 13 mil 977 MDP: Condusef", Informador.mx, 15 de febrero de 2019. Disponible en: https://www.informador.mx/economia/Fraudes-financieros-provocan-perdidas-por-13-mil-977-MDP-Condusef-20190215-0110.html.

techdirt. “Brazil E-Voting Machines Not Hacked... But Van Eck Phreaking Allowed Hacker To Record Votes, november 23, 2009. Disponible en: https://www.techdirt.com/articles/20091123/0147047048.shtml.

The Wall Street Journal. *Agencies Warn States that Internet Voting Poses Widespread Security Risks,* by Dustin Volz. May 8, 2020. Disponible para su consulta en: https://www.wsj.com/articles/agencies-warn-states-that-internet-voting-poses-widespread-security-risks-11588975848.

Sentencias y tesis de jurisprudencia:

Corte IDH. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5.

CoIDH. Caso Herrera Ulloa vs. Costa Rica. Excepciones preliminares, Fondo Reparaciones y Costas. Sentencia de 2 de julio de 2004. Serie C, N.º 107.

Caso Claude Reyes y otros Vs. Chile. Fondo, Reparaciones y Costas. Sentencia de 19 de septiembre de 2006. Serie C No 151.

CoIDH. Alegatos ante la Corte Interamericana en el caso Ricardo Canese Vs. Paraguay. Transcritos en: Corte I.D.H., Caso Ricardo Canese Vs. Paraguay. Sentencia de 31 de agosto de 2004. Serie C No. 111.

CoIDH. Caso Yatama Vs. Nicaragua. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 23 de junio de 2005. Serie C No. 127.

CoIDH. Caso Castañeda Gutman vs México. Sentencia de 6 de agosto de 2008. Excepciones preliminares, fondo, reparaciones y costas. Serie C, No. 184.

Caso Gomes Lund y otros ("Guerrilha do Araguaia") Vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 24 de noviembre de 2010.

CoIDH. Caso López-Mendoza vs. Venezuela. Sentencia de 1 de septiembre de 2011. Fondo, reparaciones y costas. Serie C, No. 232, párrafo 108

CoIDH. Caso Argüelles y otros vs. Argentina. Sentencia de 20 de noviembre de 2014. Excepciones preliminares, fondo, reparaciones y costas. Serie C, No. 288.

Sentencia 2 BvC 3/07 - 2 BvC 4/07. Tribunal Constitucional Alemán, 3 de marzo de 2009. Tribunal Constitucional Alemán.

TEPJF. MECANISMOS DE DEMOCRACIA DIRECTA. EN SU DISEÑO DEBEN OBSERVARSE LOS PRINCIPIOS CONSTITUCIONALES PARA EL EJERCICIO DEL DERECHO HUMANO DE VOTAR. Tesis XLIX/2016. Gaceta de Jurisprudencia y Tesis en materia electoral, Tribunal Electoral del Poder Judicial de la Federación, Año 9, Número 18, 2016, páginas 96 y 97.

Reportes de auditorías e informes sobre el SEI:

KIMAT. *Dictamen de Auditoría para el Instituto Electoral de la Ciudad de México,* 20 de julio de 2017, pp. 15-16.

UNAM FES Aragón. *Voto desde el extranjero bajo la modalidad electrónica – Implementación a través del Sistema de Voto Electrónico por Internet, dictamen auditoría UNAM*, julio de 2017.

UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe final de la Auditoría de Software previo a la jornada de votación y opinión.* Periodo de evaluación: 24 febrero a 30 de marzo de 2020.

UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de la Auditoría Informática realizada durante la jornada.* Periodo de evaluación: 7 al 15 de marzo de 2020.

UNAM FES Aragón Centro Tecnológico Aragón, Laboratorio de Cómputo. *Auditoría Informática al Sistema Electrónico por Internet (SEI) para el IECM. Informe de Evaluación de la Auditoría Informática (informe posterior a la jornada).* Periodo de evaluación: 15 al 17 de marzo de 2020.

Barrat, Jordi y Morales, Víctor. *Informe de Voto Electrónico*, 30 de abril de 2020.

El Voto por Internet en México:

la libertad y la secrecía del voto condicionadas

Por: Vladimir Chorny

Ciudad de México. México, octubre 2020

R3D

Red en Defensa
de los Derechos Digitales

@R3D