Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
www.juridicas.unam.mx www.bibliojuridica.org

Capítulo VII

DELITOS INFORMÁTICO-ELECTORALES EN MATERIA DE VOTO ELECTRÓNICO

Olivia Valdez Zamudio[1]

SUMARIO:

1. Introducción. 2. Voto Electrónico : Ventajas y desventajas. 3. Diferencia entre voto electrónico y voto por internet. 4. Situación en México. 5. Delitos Electorales. 6. Delitos Informáticos. 7. Voto de mexicanos en el extranjero. 8. Consideraciones Finales. 9. Fuentes de Información. ***Anexo 1****: Tipos de delitos informáticos reconocidos por Naciones Unidas.*

1 Abogada y estudiante de la maestría en Derecho Procesal Constitucionalde la Universidad Panamericana, asistente de investigación en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México UNAM, México, en el área de Derecho Electoral y Derecho de las Tecnologías de la Información y Comunicación.oz_valdez@hotmail.com

DR © 2011, Lucero Romero Lopéz

DR © 2011, Lucero Romero Lopéz

1. INTRODUCCIÓN

Tipificar conductas implícitas con el advenimiento de las nuevas tecnologías, es una tarea obligada, sancionar conductas ilícitas derivadas de la aplicación de las nuevas tecnologías a los procesos electorales y que adicionalmente puedan vulnerar la voluntad ciudadana, resulta una tarea impostergable. Esta tendencia tecnológica ahora vinculada al ejercicio de la ciudadanía, específicamente en el ámbito de la participación política, la podemos sintetizar en una frase, se trata del "nuevo horizonte tecnológico en materia electoral."[2]

Una visión hegeliana al respecto, indicaría que el mundo se encuentra en constante evolución. En efecto, la informática ha constituido el punto de partida en la renovación del propio ser humano y adicionalmente ésta, sigue ofreciéndole el punto de torque de su incesante y vertiginoso devenir evolutivo. Sobre este punto, es interesante analizar lo que sostiene Ray Kurzweil, al señalar que la especie humana emerge como creadora de tecnología y sostiene que la tecnología es la continuación de la evolución por otros medios, y es en sí misma un proceso evolutivo.[3] Lo anterior, nos lleva a establecer a priori *que renunciar a la tecnología, sería tanto como tratar de evadir la propia evolución humana, escenario inimaginable.*

2. VOTO ELECTRÓNICO: VENTAJAS Y DESVENTAJAS

Podemos entender en términos generales al voto electrónico como el*proceso enque el elector, usando las nuevas tecnologías de la información y comunicación, ejerce su derecho al sufragio.*

Beneficios:

a) Facilita el proceso electoral, ya que ofrece datos fiables y rápidos en cuanto a captación de votos y resultados.

2 La autoría de la frase corresponde al Mtro. Mauricio Sáez de Nanclares. *videtu.rAnálisis de los procesos de modernización y tecnologías para aplicar el ejercicio del voto.* Instituto Federal Electoral, México, 2003.

3 Sobre este tema, *videtur.* Kurzweill, Ray, *La era de las máquinas espirituales, cuando los ordenadores superen la mente humana*, Editorial Planeta Mexicana, México, 2000, pp 53 y ss.

DR © 2011, Lucero Romero Lopéz

b) Permite a las personas ejercer su voto desde cualquier lugar del mundo.

c) En cualquier momento el ciudadano puede verificar su elección.

d) Se obtienen y publican los resultados oficiales a pocas horas de cerrado el proceso electoral.

e) Se ahorra recursos financieros, ya que no es necesario imprimir por parte de la Autoridad Electoral las papeletas de la elección y los certificados respectivos, se constituyen menos "mesas electorales", se despliega menor logística por parte de los miembros de la Fuerza Pública.

f) Como verdadero sistema, que recoge de manera inmediata y a bajo costo, la decisión de un pueblo, los gobiernos podrían realizar las consultas populares necesarias, en un modelo de democracia participativa, en cualquier momento y lugar.

g) El uso de la urna electrónica no sólo aligerará la carga de trabajo de los funcionarios electorales, sino que podrá reducir la comisión de errores humanos, simplificar las tareas en las casillas, aumentar la rapidez en la obtención y difusión de resultados y, adicionalmente, generar importantes ahorros en la documentación y materiales electorales.

h) Existe incremento de votantes, ya que pudieran desde cualquier lugar: casa. Trabajo, escuela, ejercer su derecho.

i) No existe perdida de tiempo por parte del elector, al evitarse las largas filas en el día de la elección.

Desventajas:

a) Genera desempleo, ya que muchas personas que trabajan en el proceso electoral son despedidas o dejan de ser contratadas.

b) Es muy costoso, según lo manifestado en discusiones del Congreso del Estado de Puebla, implantarlo en el Estado ascendería a 480 millones de pesos.

c) No se garantiza la privacidad y secreto de la elección, además de que los datos si no cuentan con los candados suficientes puede ser manipulada.

d) Para una futura implantación de la urna electrónica en las elecciones formales se requiere, además de reformas legislativas, de la confianza de partidos y electores.

DR © 2011, Lucero Romero Lopéz

3. DIFERENCIA ENTRE VOTO ELECTRÓNICO Y VOTO POR INTERNET

Es conveniente hacer la diferencia entre lo que es un voto electrónico y lo que es un voto por Internet, donde en el voto electrónico, el ciudadano común debe trasladarse a un lugar que cuenta con una terminal (computadora) y un software específico, entendiendo como terminal un dispositivo mecánico-electrónico complejo o no, como es el caso de los mecanismo utilizados en las pasadas elecciones de octubre de 2005, celebradas en Argentina que hicieron uso de 4 mecanismos.

1) Lector Óptico de Boleta individual (LOB)

2) Lector Óptico de Planilla de selección múltiple (LOP)

3) Registro Electrónico con Almacenamiento digital externo(REA)

4) Registro Electrónico con Verificación impresa (REV)

Aun cuando los resultados obtenidos de pruebas piloto resultan de ayuda para el mejoramiento y corrección de defectos de logística, automatización y mejoramiento de estos mecanismos, podemos destacar dos características:

a) Positiva: El conteo se realiza de forma rápida ganando hasta 2 horas, por otra parte las personas que se encuentran fuera del país pueden votar.

b) Negativa :La libertad debe de ser apoyada por la tecnología y no de forma inversa, el costo para la implementación de estos mecanismos es elevado a nivel de hardware y software, contemplando también el costo total de propiedad donde se debe contemplar mantenimiento, licencias, soportes, capacitación.

4. SITUACIÓN EN MÉXICO

En la actualidad, la tendencia global de los organismos electorales se dirige a la utilización de la informática en la mayoría de los procedimientos electorales que por disposición legal tienen que llevar a cabo en la organización de los comicios.

DR © 2011, Lucero Romero Lopéz

En este orden de ideas, México no ha escapado a la sinergia de la informática electoral, estableciendo en algunos códigos o leyes electorales de las entidades federativas, la posibilidad de implementar subsistemas de votación electrónica. Sin embargo, nos encontramos frente a diseños institucionales jurídico-electorales parciales, es decir, ordenes jurídicos incompletos que generan asistematicidad. Lo anterior, es corroborado atendiendo a la introducción de una institución jurídica en materia electoral, que establece la posibilidad al ciudadano de sufragar a través de un procedimiento distante del sistema tradicional de voto, la cual se presenta en el sistema jurídico mexicano, como un elemento aislado de otros ordenes jurídicos, tales como; el ámbito penal y el procedimental electoral, y que por ende no permite la interpretación sistemática de esta nueva institución jurídico-electoral.

Precisemos al respecto, la noción de orden jurídico se determina por los cambios en las normas jurídicas generales del sistema[4] y es el propio sistema jurídico el cual cuenta con una serie de cualidades lógico-formales,[5] entre las que destacan: la coherencia y completitud. En realidad, la coherencia normativa se distingue por la compatibilidad de un orden jurídico con ordenes jurídicos diversos, y en este sentido, la completitud indica la totalidad de presupuestos jurídicos, es decir, la ausencia de vacios normativos o lagunas legales. En razón de lo que precede, y efectuando un análisis normativo de la institución sustentada en "subsistemas de votación electrónica", resulta que su integración normativa constituye un orden júridico-electoral parcial o asistemático, al menos en nuestro país, en virtud de que la norma electoral solamente se encuentra dispuesta u orientada a posibilitar la recepción de la votación a través de medios informáticos, sin considerar en lo más mínimo su completitud, coherencia o interdependencia con el derecho penal y el derecho procesal, específicamente éste último, en el ámbito de los medios impugnativos en materia electoral.

Lo anterior, es posible sintetizarlo formulando el siguiente cuestionamiento; ¿están debidamente previstos en la legislación mexicana, tipos penales-electorales en los que jurídicamente pudieran encuadrarse acciones u omisiones humanas; con motivo de la utilización de subsistemas de votación electrónica?. Una primera respuesta, negativa por cierto, expone al menos un vacío normativo en la esfera de los delitos electorales en México, y simultáneamente exhibe un posible déficit del principio de legalidad en materia electoral.

4 Serna de la Garza, José María. *Estado de derecho y transición jurídica*, Ed. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, 2002, pp 93 y ss.

5 Serna de la Garza, José María. Op. Cit. p. 96

DR © 2011, Lucero Romero Lopéz

En el ámbito de los dogmas penales, la idea de estricta legalidad[6] nos remite al siguiente principio jurídico: nullum crimen, nulla poena sine lege, *mismo que cobra vigencia al establecer que una pena sólo debe aplicarse como consecuencia de un delito, en el entendido que tanto la pena y el delito se encuentren debidamente previstos en la legislación; y es precisamente aquí el problema, debido a que en el contexto jurídico mexicano se carece de tipos penales-electorales* ex profeso, *situación que elude por completo la idea de estricta legalidad.*

5. DELITOS ELECTORALES

E*n las siguientes líneas, es prudente al menos, citar dos aproximaciones conceptuales ¿qué es un delito electoral?, y adicionalmente ¿qué es un delito informático?, para posteriormente establecer la conjunción de ambos (informático-electoral), clasificándolo como un "delito de naturaleza jurídica compleja."*[7]

El término delictum electio, *en su concepción etimológica,*[8] se precisa como "la falta suscitada durante una elección", sin embargo, el concepto etimológicamente considerado es restringido en cuanto a su alcance. Al respecto, con mayor precisión, una primera definición acerca de los delitos electorales, la ofrece el investigador Arturo Zamora, considerando en su perspectiva que se trata de "descripciones típicas por medio de las cuales se intenta tutelar el proceso electoral, sancionando los comportamientos que impiden o dificultan la libertad de decisión de los electores, o falsean el resultado electoral."[9]

---

6 Castellanos, Fernando. *Lineamientos elementales de derecho penal,* Editorial Porrúa, México, 1987, p.80.

7 En este tema se sigue de cerca la clasificación de los delitos formulada por Fernando Castellanos. *Op. Cit.*, pp. 141 y ss.
Sobre el particular, el juspenalista indica que los "delitos complejos" son aquellos en los cuales la figura jurídica consta de la unificación de dos infracciones, cuya fusión da nacimiento una figura delictiva nueva, superior en gravedad a las que la componen, tomadas aisladamente. Al respecto, Edmundo Mezger citado por Castellanos, estima que el delito complejo se forma de la fusión de dos o más. Adicionalmente, sostiene que no es lo mismo delito complejo que concurso de delitos. En el delito complejo la misma ley en un tipo crea el compuesto como delito único, pero en el intervienen dos o más delitos que pueden figurar por separado; en cambio, en el concurso, las infracciones no existen como una sola, sino separadamente, pero es un mismo sujeto quien las ejecuta.

8 *Breve diccionario latín/español,* Editorial Porrúa, México, 2004, p 148.

9 Zamora Jiménez, Arturo. *Delitos electorales,* Ángel editor, México, 2003, p.198.

DR © 2011, Lucero Romero Lopéz

Una característica esencial de los delitos electorales es su comisión intra- proceso, es decir, la temporalidad en la que tienen verificativo una serie de conductas ilícitas, se contrae exclusivamente durante el periodo comicial. Por otra parte, es importante destacar que la comisión de los delitos electorales, y específicamente los informático-electorales solamente pueden ser cometidos a través de sujetos activos diferenciados o especializados, los cuales cuentan con una serie de características en cuanto a formación técnica o especializada, misma que les permite desarrollar ciertas habilidades informáticas.

6. DELITOS INFORMÁTICOS

En lo que concierne a los delitos informáticos, el doctor Julio Téllez, los define como una "serie de actos ilícitos en que se tiene a las computadoras como instrumento o fin". Añade, que algunas de las características principales, por sólo citar algunas de las múltiples que enumera este autor, son:[10]

a) Que fundamentalmente se catalogan como delitos de cuello blanco, esto es, que sólo un reducido grupo de personas está en condiciones de cometerlos (personal técnico).

b) Que presentan grandes dificultades para demostrar su comisión, en razón de su compleja naturaleza de orden técnico.

A manera de síntesis, la clasificación de estos tipos penales informáticos obedece a lo que acertadamente el Consejo de la Unión Europea ha conceptualizado como "delincuencia de alta tecnología".[11] En este tenor, la respuesta ha sido, la adopción de la Convención sobre Cybercrimen signada por el Consejo de la Unión Europea, la cual constituye una iniciativa multinacional destinada a enfrentar el incremento de conductas delictivas que se suscitan a través de medios electrónicos.

Sobre el particular, el Profesor Jeffrey F. Addicott, investigador de la Universidad de Saint Mary en Texas, ha sostenido que con relación a los crímenes cibérneticos, en el léxico de la terminología informática, existen tres tipos de delincuentes cibernéticos: *script-kiddies, hackers*[12] y crackers.[13]

10 Téllez Valdés, Julio. *Derecho informático*, Editorial Mc Graw Hill Interamericana, 3ª. Edición. México, 2004, p. 163.

11 Recomendación del Consejo de 25 de junio de 2001 sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología. *Diario Oficial de las Comunidades Europeas*. 200/C 187/02.

DR © 2011, Lucero Romero Lopéz

Ahora bien, ante la presencia de una figura delictiva nueva de naturaleza compleja, que hemos definido como delitos informático-electorales, es prudente enumerar los sujetos activos que penalmente pueden incurrir en estas conductas delictivas cibernético-comiciales, en esta hipótesis normativa se encontrarían: los funcionarios de casilla, los ciudadanos, los candidatos, los representantes de partidos políticos y el personal técnico que auxilia a la autoridad electoral. En esta lógica, los sujetos pasivos en quienes podrían recaer estas conductas criminógenas serían: el Estado y la ciudadanía, los partidos políticos y los candidatos.

En una eventual descripción legal de los delitos informático-electorales, los elementos del delito estarían constituidos por: a) la alteración, sustracción, apropiamiento indebido o destrucción de elementos o sistemas informáticos; b) que el autor(es) transgreda el derecho de sufragio; y c) el nexo causal entre el primer y segundo elemento. Estas constitutivas[14], resultaran indispensables a manera de conjunción en la integración del tipo penal.

En esta tesitura, los tipos penales en su redacción normativa deberán prever algunas hipótesis, sancionando las siguientes conductas antijurídicas cibernético-comiciales:

a) Al que se introduzca sin autorización alguna, en los sistemas informáticos de manera previa, durante o después de la jornada electoral con el propósito de causar daños mediante la alteración de la información, la sustracción de la misma e inclusive introduciendo programas informáticos que modifiquen los resultados electorales;

b) Así también, el que sin mediar autorización diseñe o transmita programas informáticos que tengan como finalidad bloquear sis-

12 En torno al tema, *videtur*. Sterling, Bruce. *La caza de hackers*, Bantam Books, edición electrónica, 1994.

13 González, Verónica, "Qué es el ciberterrorismo", Revista Mundo Legislativo, México, Año I, núm. 1, 2005.
En este tema, el profesor Jeffrey F. Addicott, indica que los *script-kiddies* son criminales de informática de bajo nivel, generalmente descargan diferentes paquetes y herramientas de informática de Internet y las utilizan para explotar las debilidades en seguridad de un sistema. Por otra parte, el *hacker* es más sofisticado y utiliza sus habilidades en informática para penetrar sistemas seguros. Respecto al *cracker*, señala que es el delincuente informático más peligroso, en virtud de que ataca el sistema informático con propósitos verdaderamente criminales que implican chantaje, espionaje o creadores de virus informáticos.

14 Una exposición notable sobre el particular *videtur*. González de la Vega, Francisco, *Derecho penal mexicano*, Editorial Porrúa, 22°. edición. México, 1988, p. 250.

DR © 2011, Lucero Romero Lopéz

temas informáticos; utilizados durante la jornada electoral y la transmisión de los resultados electorales, inclusive aquéllos que se generen por parte de la autoridad electoral de manera preliminar;

c) Al que viole la secrecía del voto, modificando algoritmos que permitan descifrar el sentido de la votación del elector;

d) Al que pretenda suplantar la identidad del votante a través de medios biométricos o informáticos;

e) A quien altere, sustituya, dañe o destruya insumos o dispositivos informáticos que se utilicen durante el día de la elección;

f) A quien utilice o altere indebidamente códigos de accesos de la votación, o bien de control de los dispositivos informáticos utilizados durante la jornada electoral;

g) Al que genere la apertura y cierre de manera dolosa de un sistema informático fuera de los plazos establecidos por las normas electorales;

h) Al que permita que un ciudadano emita su voto, entregándole de manera indebida códigos de acceso de votación; y

i) Al que utilice o modifique sin autorización debida cualquier elemento criptográfico de los sistemas de votación electrónica a utilizarse durante la jornada electoral.

En cuanto a la punibilidad[15], partiendo de la teoría del juspenalista Fernando Castellanos, tratándose de delitos de naturaleza compleja que presentan la unificación de dos o más conductas antijurídicas y cuya fusión da origen a esta figura delictiva de reciente creación, habría que considerar su superior gravedad a lo que inicialmente es normado aisladamente como delitos informáticos y delitos electorales. En síntesis, no solamente se actualiza la comisión de un delito de alta tecnología, sino que adicionalmente vulnera el derecho de sufragio, situación que resulta doblemente grave y habría que considerar ambos factores de comisión en el merecimiento de las penas correspondientes.

Contar con un marco normativo integral en el ámbito del derecho penal electoral, que regule delitos de naturaleza jurídica compleja como lo son; los delitos informáticos-electorales, permitirá, sin lugar a dudas un proceso de adecuación típica[16] que mediante acciones tuitivas, resguarde

15 Entendiendo a ésta como el merecimiento de la pena en función de la realización de una conducta antijuridica.

DR © 2011, Lucero Romero Lopéz

el derecho de sufragio del ciudadano, otorgue garantías hacía los partidos políticos y garantice la función estatal de organizar comicios, en el afán democrático de originar certeza y legalidad, ambos, valores esenciales que tutela el derecho.

7. VOTO DE MEXICANOS EN EL EXTRANJERO

a. Marco teórico

Para abordar este tema, queremos empezar enfatizando dos aspectos fundamentales y básicos: se ha calculado que, a la fecha, son cerca de 10 millones de ciudadanos mexicanos que residen en el extranjero. El 95% radica en los EUA y en Canadá. El segundo de estos aspectos es que de 10 millones, solamente 3.5 cuentan con credencial para votar expedida por el Registro Federal de Electores. Para delimitar esta exposición omitiremos al principio aspectos relacionados con costos y la conveniencia de su implementación, y nos centraremos precisamente en aspectos técnico-jurídicos-penales, que deben contemplarse para el caso de que se otorgue el derecho al voto de los mexicanos en el extranjero. Establecer los medios de protección en la norma penal para evitar la compra y coacción del voto, ya que pueden presentarse casos en los cuales se busque violentar o atentar contra la libertad del voto bajo cualquier medio, ya sea ofreciendo beneficios económicos o en especie a los votantes en el extranjero. Entre los desafíos más importantes para poder modernizar los sistemas electorales están el conseguir recursos económicos para la adquisición de equipos nuevos y modernos, la instalación de programas y aplicaciones tecnológicas así como la capacitación del personal de la institución electoral que utilizará la tecnología en los distintos países. Asimismo, será muy importante lograr la adaptación de los países a los nuevos requerimientos tecnológicos de los procedimientos automatizados, por ejemplo:

> contar con normas legales modernas, es decir, adecuadas para la incorporación tecnológica en el régimen electoral y para que faciliten el ejercicio del sufragio al elector;
>
> es necesario mejorar las capacidades y niveles de eficacia de los partidos políticos para el cumplimiento de sus funciones y especialmente para el ejercicio de gobierno;

16 En tal sentido, *videtur*. Castellanos, Fernando., *Op.Cit.* p.81.

DR © 2011, Lucero Romero Lopéz

establecer buenas relaciones entre partidos políticos, sociedad civil organizada, medios de comunicación, sector privado y ciudadanía en general.

Alterar por cualquier medio las claves necesarias para emitir el voto electrónico o introducirse en la red sin importar el objeto de dicha conducta o pretender introducir algún virus informático en la línea electrónica o en las bases de datos en cualquier unidad remota así como en los sistemas de concentración de datos pueden concurrir en los delitos informáticos y además, deberá valorarse por parte del Poder Legislativo en relación a estas conductas cuáles deberán agravarse de acuerdo a la calidad del sujeto activo. Puede ser el caso de un servidor público o un funcionario electoral que divulgue o de a conocer a cualquier persona las medidas de seguridad implementadas para la recepción de la votación o cuando aprovechándose de la información con que cuente, altere los resultados distorsionando el desarrollo de la votación.

En caso de optarse por la recepción de la votación en casillas electrónicas, eliminando el uso de boletas de papel, deben crearse tipos penales que salvaguarden la integridad de los registros electrónicos y de la certeza de la entrega de las autoridades electorales, sancionando a los funcionarios electorales y a los servidores públicos que intervengan en la jornada electoral.

b. Marco jurídico

Con respecto a la votación de Mexicanos en el extranjero, el Código Federal de Instituciones y Procedimientos Electorales (COPIFE) fue modificado el 30 de junio de 2005, en cuanto al uso de medios electrónico y protección de datos personales a saber :

Artículo 279...
5. Para fines estadísticos y de archivo, el Instituto conservará copia, en medios digitales, por un periodo de siete años, de las listas nominales de electores residentes en el extranjero.

Datos personales

Artículo 280...
3. En todo caso, el personal del Instituto y de los partidos políticos están obligados a salvaguardar la confidencialidad de los datos personales contenidos en las listas nominales de electores residentes en el extranjero. La Junta General Ejecutiva dictara

DR © 2011, Lucero Romero Lopéz

los acuerdos e instrumentara las medidas necesarias para tal efecto.

Artículo 281 ...
1. Los partidos políticos, a través de sus representantes en la Comisión Nacional de Vigilancia, tendrán derecho a verificar las listas nominales de electores residentes en el extranjero a que se refiere el inciso b del artículo anterior, a través de los medios electrónicos con que cuente la Dirección Ejecutiva del Registro Federal de Electores.

Artículo 287...
1. La Junta General dispondrá lo necesario para:
a. Recibir y registrar, señalando día, los sobres que contiene la leyenda electoral, ...
b. Colocar la leyenda "votó" al lado del nombre del elector en la lista nominal correspondiente; lo anterior podrá hacerse utilizando medios electrónicos.

Artículo 290...
2. El Consejo General podrá determinar el uso de medios electrónicos para el cómputo de los resultados y la elaboración de actas en informes relativo al voto de los electores residentes en el extranjero. En todo caso, los documentos así elaborados deberán contar con firma.

Artículo 89 ...
1. l) Establecer un mecanismo para la difusión inmediata en el Consejo General, de los resultados preliminares de las elecciones de diputados, senadores y Presidente de los Estados Unidos Mexicanos; para este efecto se dispondrá de un sistema de informática para recabar los resultados preliminares.

Debemos recordar que parte del debate de estas reformas se centró en el método que se utilizaría para la emisión de estos votos. Opinamos como equipo que si perdemos la oportunidad como país de utilizar los medios electrónicos para este fin, más allá de la factibilidad técnica, aquí vemos que el punto que definió todo fue el de la factibilidad política. Nos queda claro que técnicamente no hay impedimento pero no se llegó al acuerdo político necesario. Aún y con esto, nos llama la atención la cantidad de menciones que se hacen a los medios electrónicos y/o digitales, al menos cuatro veces se menciona el término y el párrafo que menciona la protección de datos personales. Un dato curioso que nos llama la atención es que se menciona al menos 100 veces la palabra "cómputo" en el texto del COPIFE, sin embargo no se define el término, algo raro que

DR © 2011, Lucero Romero Lopéz

desde nuestro punto de vista y sin ser abogados hemos encontrado que es muy importante definir con precisión los términos para dar claridad a las leyes. Pues bien una ves revisada la legislación del IFE podemos decir que a nivel Federal no es posible utilizar desde el punto de vista legal o jurídico urnas electrónicas y/o redes públicas como Internet para la emisión del voto, pero si se define el uso de medios electrónicos para el control y conteo de los mismos, inclusive el Programa Preliminar de Resultados Electorales (PREP) utiliza Internet para el despliegue de la información.

8. CONSIDERACIONES FINALES

Algunas recomendaciones en materia de delitos informático-electorales pueden ser:

implantación de cualquier tecnología debe de hacerse con mucha prudencia y sobre todo haciendo una correcta elección de los centros de votación.

mecanismos que impidan votar más de una vez a un mismo ciudadano.

presentación equitativa de las formaciones políticas.

medidas adecuadas que compensen la deficiente alfabetización digital de los ciudadanos.

Es por ello que todo proyecto de implantación del voto electrónico debe contar con un programa de formación y asistencia que logre que cada ciudadano pueda acceder al sistema con plenas garantías. Esto quiere decir que se diseñe un plan de trabajo a medio y largo plazo para que la introducción de estas herramientas no sorprenda a la población. El día de la votación, deberán existir asimismo equipos de ayuda que puedan solventar las dudas que surjan en ese momento

El proceso electoral electrónico, también conocido como democracia electrónica y/o e-voting es algo que inevitablemente tendrá que llegar. Los retos son muy similares a los que afronta el comercio electrónico y se debe de legislar en diversos sentidos, en materia de protección de Datos personales, en Firma electrónica y en tipificar como delitos electorales algunos otros factores, como por ejemplo sabotaje de elección, con el fin de que los sistemas democráticos sean mas sólidos y rescatar al sistema democrático de lo que parece ser su cáncer, el abstencionismo y la

DR © 2011, Lucero Romero Lopéz

desconfianza. Podemos decir que la tendencia mundial en los países democráticos es la de organizar elecciones electrónicas y dar oportunidad, en este mundo globalizado, de que sus ciudadanos dispersos en varias partes del mundo elijan a sus mandatarios.

Podemos decir que aún estando en países con sistemas electorales fiables, la introducción de nuevas tecnologías se podría hacer pero con mucha prudencia para tener como resultado la constante participación ciudadana.

Por otro lado es de suma importancia recalcar que muchos estados realizan enormes esfuerzos por aumentar la fiabilidad de su logística electoral, pero desgraciadamente se topan con la corrupción, el desinterés y con el analfabetismo de segmentos importantes de la población. ¿Puede el voto electrónico aportar elementos positivos a esta preocupante situación? La respuesta es sencilla, el voto electrónico, aún en los casos más extremos, puede aportar aspectos positivos. Existen casos sui géneris, como el de nuestro país en el que el fenómeno migratorio es multitudinario, algunos lo llaman inclusive éxodo.

En estos casos tan relevantes, se vuelve prioritario el marco jurídico que de certeza a los actores políticos y que regule el fondo y la forma de la elección. El voto electrónico puede ser enormemente útil para determinados sectores de la sociedad como por ejemplo los ciudadanos discapacitados, residentes ausentes e incluso, en casos como el de los invidentes, los dispositivos electrónicos podrían facilitar su votación presencial de forma autónoma. Algunos modelos de voto electrónico –no todos—simplifican sobremanera tal dinámica y permiten aventurar un futuro en el que puedan ofrecerse a los ciudadanos mayores instrumentos de participación. Es necesario señalar que la tasa de votación aumentaría con la implantación de procedimientos electrónicos, ya que por ejemplo los jóvenes que la mayoría de las veces se abstienen de votar, con este tipo de tecnologías es posible que se animen y lo hagan más frecuentemente. En cuanto al proceso tradicional, el mayor avance que destacamos es el de la confianza de la ciudadanía y el acuerdo político alcanzado para incorporar medios electrónicos.

Los ajustes a las legislaciones deben de ir encaminados a la inclusión de métodos electrónicos, siendo específicos y claros en cuanto a los instrumentos tecnológicos que se han de utilizar, no es raro que en prácticamente todos los procesos electrónicos que se han llevado a cabo en el mundo la principal característica o tópico es el rubro de la seguridad. En el aspecto de la seguridad, creemos que debemos de tomar en cuenta las legislaciones en materia de protección de datos personales para evitar que los padrones electores sean comercializados (tal y como vimos durante

DR © 2011, Lucero Romero Lopéz

el curso el caso de la venta del padrón mexicano a una empresa estadounidense). La legislación en materia de firma electrónica para aprovechar que se legisle en materia de certificados digitales y otras tecnologías así como algunas otras leyes que le den certeza a los mecanismos electrónicos.

Nos queda claro que técnicamente no hay impedimento y deben existir mayores acuerdos políticos y opinamos como equipo que si perdemos la oportunidad como país de utilizar los medios electrónicos para este fin, perderemos un paso fundamental en la evolución como una sociedad eficiente, capaz de manejar sus asuntos sociales de manera más practica, rápida y exacta. Consolidarnos como una sociedad progresista en términos de medios, y tradicionalista en términos de la protección de valores democráticos como libertad, honestidad, eficacia, flexibilidad al cambio. Que sean la construcción y procuración de valores nuestros mas grandes ideales con medios que sirvan para alcanzarlos como lo son los medios electrónicos. Sean ellos nuestros mas cercanos aliados para reflejar una voluntad ciudadana, plural, incluyente y representativa ávida de ejercer su libertad de elección pero sobre todo, de encontrar personajes indicados que la hagan valer.

9. FUENTES DE INFORMACIÓN

CALAMANDREI, Piero. *Elogio de los jueces escrito por un abogado*. Editorial Oxford University Press. México, 2000.

CASTELLANOS, Fernando. *Lineamientos elementales de derecho penal*. 24ª. edición. Editorial Porrúa. México, 1987.

GONZÁLEZ, De la Vega Francisco. *Derecho Penal Mexicano*. 22ª. edición. Editorial Porrúa. México, 1988.

KURZWEIL, Ray. La era de las máquinas espirituales. 1ª. reimpresión. Editorial Planeta Mexicana, México, 2000.

PÉREZ, Valera Víctor Manuel. *Deontología jurídica, la ética en el ser y quehacer del abogado*. Editorial Oxford University Press. México, 2002.

ROMERO, Rodolfo y TELLEZ, Julio, *Voto Electrónico, Derecho y otras Implicaciones*, Instituto de Investigaciones Jurídicas, UNAM, México, 2010

DR © 2011, Lucero Romero Lopéz

ZAMORA, Jiménez Arturo. *Delitos electorales*. Ángel Editor. México, 2000.

TÉLLEZ, Valdés Julio. *Derecho informático*.4ª. edición. Editorial Mc Graw Hill. México, 2009.

Diccionarios consultados

Breve diccionario Latín/Español. 3ª. edición. Editorial Porrúa. México 2004.

Legislación

Código Penal Federal. Edición electrónica de la Cámara de Diputados del H. Congreso de la Unión, México, 2010. http://www.cddhcu.gob.mx/

Código Federal de Instituciones y Procedimientos Electorales . Edición electrónica de la Cámara de Diputados del H. Congreso de la Unión, México, 2010. http://www.cddhcu.gob.mx/

Anexo 1:
TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR NACIONES UNIDAS

FRAUDES COMETIDOS MEDIANTE MANIPULACIÓN DE COMPUTADORAS

MANIPULACIÓN DE LOS DATOS DE ENTRADA:

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

DR © 2011, Lucero Romero Lopéz

MANIPULACIÓN DE PROGRAMAS:

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

MANIPULACIÓN DE LOS DATOS DE SALIDA:

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

MANIPULACIÓN INFORMÁTICA APROVECHANDO REPETICIONES AUTOMÁTICAS DE LOS PROCESOS DE CÓMPUTO:

Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

FALSIFICACIONES INFORMÁTICAS

COMO OBJETO:

Cuando se alteran datos de los documentos almacenados en forma computarizada.

COMO INSTRUMENTOS:

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documen-

DR © 2011, Lucero Romero Lopéz

tos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS

SABOTAJE INFORMÁTICO

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

VIRUS:

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

GUSANOS:

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

BOMBA LÓGICA O CRONOLÓGICA:

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga

DR © 2011, Lucero Romero Lopéz

lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS:

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

PIRATAS INFORMÁTICOS O HACKERS:

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL:

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

DR © 2011, Lucero Romero Lopéz