ARTÍCULO DE OPINIÓN

La inconclusa reforma al Código Penal Federal en materia de delitos informáticos

Levet Rivera, Carlos Enrique
Universidad Veracruzana, México
clevet@uv.mx

Macgluf Issasi, Arturo
Universidad Veracruzana, México
amacgluf@uv.mx

Espinoza Maza, Jonathan de Jesús
Universidad Veracruzana, México
jespinoza@uv.mx

Fragoso Teran, Juan Manuel
Universidad Veracruzana, México
juafragoso@uv.mx

Resumen - La aparición de las Tecnologías de Información y Comunicación en los años noventa, motivó reformas al Código Penal Federal Mexicano para incluir la figura de delito informático; a la fecha no se ha actualizó dicha ley en esa materia, por lo que, no se puede sancionar a las personas por conductas no previstas en la legislación penal, quedando desfasado dicho delito.

Palabras Clave: Tecnología; Computación; Ciencias de la Información; Delito Cibernético; Computación; Suplantación de identidad; Legislación;

Abstract - The emergence of Information and Communication Technologies in the nineties, encouraged reforms to the Mexican Federal Criminal Code to include the concept of cybercrime. So far, this law has not been updated in this area. Therefore, people cannot be punished for not listed behaviors in the criminal legislation, being that offense out of date.

Keywords: Technology; Computing; Information Sciences; Cybercrime; Computing; Impersonation of identity; Legislation;

Ante el avance tecnológico por el uso de las computadoras personales y el creciente acceso a la internet para navegar en la supercarretera de la información conocida como la World Wide Web (www), y debido a las presiones de organismos internacionales para legislar en materia de ciberdelitos, el 17 de mayo de 1999, el Ejecutivo Federal publicó en el Diario Oficial de la Federación el Decreto por el cual se reforman y adicionan diversas disposiciones al Código Penal Federal, dentro de los cuales destaca: la adición del Capí-

Interconectando Saberes, 2019
ISSN: 2448-8704
Fecha de Recepción: 15 de junio de 2019
Fecha de Aceptación: 28 de junio de 2019
Fecha de Publicación: 30 de junio de 2019
DOI: https://doi.org/10.25009/IS.V0I7.2628

tulo II, denominado, "Acceso ilícito a sistemas y equipos de informática", que comprende los artículos 211 bis 1 al 211 bis 7, teniendo como finalidad tipificar como delito la conducta de aquellas personas que sin autorización modifiquen, destruyan o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, que sean tanto de particulares, como del Gobierno Federal, del Sistema Financiero y de Seguridad Pública. Con la anterior reforma, el Gobierno Federal encabezado por el entonces presidente Ernesto Zedillo Ponce de León, pregonaba que se tenía legislación penal federal vanguardista.

Dicha reforma no ha sido tocada hasta la fecha y continúa teniendo el mismo tipo penal, aun y cuando las conductas desplegadas con el uso de las tecnologías de la información y comunicación son más dañinas y peligrosas, dejando a los usuarios de estas en clara desprotección como se verá más adelante. Los diputados federales han realizado dos intentos de reforma y adición a la legislación penal federal pero no ha encontrado apoyo en los demás legisladores, es por ellos que el presente trabajo se denominó como la inconclusa reforma al Código Penal Federal en materia de delitos informáticos.

A nivel internacional vale la pena recordar que la Organización de la Naciones Unidas (ONU) celebró el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente que se llevó a cabo en Viena, capital de Austria, los días del 10 al 17 de abril de 2000. En dicha reunión se hizo un análisis de las repercusiones negativas que se han tenido por el uso de las computadoras y el abuso del Internet. Reconoce, además, que los delincuentes de la informática son tan diversos como sus delitos. Al respecto, señala:

> *"Los delincuentes cibernéticos pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en «paraísos informáticos» -o sea, en países que carecen de leyes o experiencia para seguirles la pista." (Organización de las Naciones Unidas, 2000)*

Otra experiencia internacional que vale la pena incluir en esta investigación, es la lucha contra la Ciberdelincuencia que se generó en el Consejo de Europa y que es generalmente conocido como Convenio de Budapest. Dicho convenio debe este nombre porque se firmó en la ciudad de Budapest capital de Hungría, el 23 de noviembre de 2001 y entró en vigor en Europa el 01 de julio de 2004. Este instrumento europeo destaca el catálogo de conductas desplegadas a través de sistemas informáticos que son considerados como Ciberdelitos.

A pesar de que los Estados Unidos de Norteamérica, Canadá, Japón y China participaron como observadores en la redacción de este convenio y el primer país lo ratificó en 2007, México no los ha tomado en cuenta.

Otra experiencia internacional de la lucha contra la ciberdelincuencia es la llevada a cabo por la Unión Internacional de Telecomunicaciones (UIT por sus siglas en castellano y ITU por sus siglas en inglés), organismo especializado de la Organización de la Naciones Unidas en materia de telecomunicaciones, quien en el mes de abril del año 2009, publicó el libro: “El Ciberdelito: Guía para los países en desarrollo”. Dicha obra contiene gran parte del contenido del Convenio de Budapest, además de hacer una explicación muy detallada de cada conducta considerada como delictiva e incluir otras más que el referido Convenio no contempla.

Después de describir los esfuerzos que han llevado a cabo los organismos internacionales en diversos países, vale la pena reflexionar que se está haciendo en nuestro país y si, además, las conductas y repercusiones han sido similares a las reportadas en las investigaciones de dichos entes especializados.

Por su parte la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros por sus siglas CONDUCEF en su análisis estadístico reportó que los delitos cibernéticos han aumentado considerablemente ya que en 2013 representaban el 12% de las quejas presentadas, mientras que

en el 2018 aumentó al 59% destacando el fraude y el robo de identidad como las más frecuentes. El monto reclamado de los fraudes cibernéticos ascendió a $9,517.2 mdp; se bonificó sólo el 55% y 88 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario. (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, 2019).

A nivel interno no se debe dejar pasar inadvertido que la Comisión de Justicia de la LXI Legislatura de la Cámara de Diputados, en el año 2012, elaboró y aprobó un dictamen con proyecto de Decreto que reforma y adiciona diversas disposiciones al Código Penal Federal, en materia de delitos en contra de medios o sistemas informáticos. Dicho documento fue formulado con motivo de las propuestas de reforma que presentaron los diputados Juan José Guerra Abud, Rodrigo Pérez-Alonso González y Canek Vázquez Góngora misma que fue publicada en la Gaceta Parlamentaria, año XV, número 3480-III, el día miércoles 28 de marzo de 2012, la cual fue aprobado por el pleno de la Cámara de Diputados y turnado a la Cámara de Senadores para su discusión y en su caso aprobación, lo cual nunca fue turnada al pleno sin explicación alguna, fue archivada. Dentro de las principales características de esta propuesta de reforma al Código Penal, destacan tipificar como delito las conductas resaltadas como Ciberdelitos en las convenciones de la ONU, el Convenio de Budapest y las recomendaciones de la UIT.

De haberse aprobado hubiera ampliado los tipos penales que hoy no están vigentes en nuestro país en materia de ciberdelitos, lamentablemente seguimos como hasta 1999, en México no se pueden sancionar las conductas consideradas como delictivas en otros países en materia de delitos informáticos.

Es importante tomar en cuenta que de acuerdo con nuestro sistema jurídico, el Ius Puniendi que dispone el Estado mexicano debe respetar el principio de legalidad previsto en el artículo 14 constitucional; bajo este principio, no puede haber delito sin ley o tipo penal, (nullum crimen nulla poena sine lege), consecuentemente, las conductas desplegadas no pueden ser

sancionadas de acuerdo con lo expresado. Bajo esta tesitura si la conducta no está prevista como delito en la legislación penal no puede ser sancionada. Además, la norma debe ser clara y contundente para que no quede la discrecionalidad y arbitrio del juzgador la aplicación de la sanción correspondiente. Dice la Segunda Sala de la Suprema Corte de Justicia de la Nación, que la exacta aplicación de la ley penal, obliga a la autoridad legislativa a emitir normas claras en las que se precise la conducta reprochable y la consecuencia jurídica por la comisión de un ilícito, a fin de que la pena se aplique con estricta objetividad y justicia; que no se desvíe ese fin con una actuación arbitraria del juzgador, ni se cause un estado de incertidumbre jurídica al gobernado a quien se le aplique la norma, con el desconocimiento de la conducta que constituya el delito, así como de la duración mínima y máxima de la sanción, por falta de disposición expresa. (Semanario Judicial de la Federación y su Gaceta, 2006)

Cuando se aprobó la reforma al Código Penal Federal se tenía un modelo penal diferente, hoy en día a partir de la reforma constitucional de 2008, se tiene un sistema procesal acusatorio y oral en donde las pruebas son contundentes para demostrar el hecho delictivo, por lo cual pareciera que al Estado mexicano no le interesa realizar acciones para proteger a los usuarios de las tecnologías de la información y comunicación. (Villanueva, 2015)

Los juristas mexicanos, no se ponen de acuerdo en la concepción y definición cuando abordan el tema de los delitos informáticos, ejemplo de ello las siguientes definiciones:

Jorge Navarro Islas expone la siguiente definición: “toda conducta típica, antijurídica y dolosa que utilice como medio comisivo o como fin un sistema de procesamiento de información digital, o que involucre al mismo como instrumento de almacenamiento de pruebas” (Navarro Islas, 2005)

Por su parte Julio Téllez Valdés ofrece la siguiente definición: “actitudes ilícitas que tienen a las computadoras como instrumento o fin” (concepto atípico) o las “conductas típicas, antijurídicas y culpables

que tienen a las computadoras como instrumento o fin" (concepto típico). (Téllez Valdés, 2009)

Para Gabriel Andrés Cámpoli, los delitos informáticos "son aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos." (Andrés Cámpoli, 2004)

El jurista Alberto E. Nava Garcés, propone la siguiente concepción: "toda conducta ilegal que involucra el procesamiento automático de datos y/o la transmisión de éstos". (Nava Garcés, 2007)

El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el *phishing*, los virus, spyware, ransomware o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas". (Avast, 2019)

La empresa estadounidense CISCO SYSTEMS dedicada principalmente a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones, anualmente emite un informe sobre Ciberseguridad, para reportar las principales amenazas a las que se enfrentan los usuarios de Tecnologías de la Información y Comunicación (Tic's). Para el año 2018 el reporte anual destaca lo siguiente (Cisco, 2018) : La evolución del malware ha hecho que las empresas antivirus se vean rebasados por la complejidad de los software maliciosos como el ransomware o secuestro de datos, tráfico web malicioso encriptado, amenazas de correo electrónico, tácticas de evasión de sandbox, abuso de servicios en la nube y otros recursos legítimos, ataques IoT y DDoS, vulnerabilidades y parches, aspectos que se comentará a continuación.

El creciente volumen de tráfico web encriptado, tanto legítimo como malicioso, crea aún más desafíos y confusión para los defensores que intentan identificar y monitorear amenazas potenciales. La encriptación está destinada a mejorar la seguridad, pero también proporciona a los actores malintencionados una poderosa herramienta para ocultar

la actividad de comando y control (C2), lo que les brinda más tiempo para operar e infligir daños.

El correo electrónico malicioso y el correo no deseado siguen siendo herramientas vitales para que los adversarios distribuyan malware porque llevan las amenazas directamente al punto final. Al aplicar la combinación correcta de técnicas de ingeniería social, como *phishing* y enlaces maliciosos y archivos adjuntos, los adversarios solo tienen que sentarse y esperar a que los usuarios desprevenidos activen sus *exploits*[1].

Los adversarios se están convirtiendo en expertos en el desarrollo de amenazas que pueden evadir entornos de *sandboxing*[2] cada vez más sofisticados.

A medida que las aplicaciones, los datos y las identidades se trasladan a la nube, los equipos de seguridad deben gestionar el riesgo que implica perder el control del perímetro de la red tradicional. Los atacantes se están aprovechando del hecho de que los equipos de seguridad tienen dificultades para defenderse de la evolución y la expansión de entornos cloud[3] y IoT[4]. Una razón es la falta de claridad sobre quién es exactamente el responsable de proteger esos entornos.

Parecería que todos los diputados son indiferentes ante los cambios tecnológicos, sin embargo, no es así, recientemente la Comisión de Justicia de la Cámara de Diputados preparó el Dictamen para Declaratoria de Publicidad del

1. Un exploit es un ataque poco ético o ilegal que se aprovecha de las vulnerabilidades de las aplicaciones, las redes o el hardware. Este ataque se suele materializar en software o código que tienen como objetivo obtener el control de un sistema informático o robar datos guardados en una red.

2. Es un mecanismo para ejecutar programas con seguridad y de manera separada. A menudo se utiliza para ejecutar código nuevo, o software de dudosa confiabilidad proveniente de terceros.

3. Conocida también como servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente "la nube", permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

4. Internet of Things o el famoso IoT, tiene como objetivo conectar el máximo de objetos que nos rodean, entre ellos y con nosotros mismos. En términos prácticos, significa que estamos rodeados de tecnología inteligente que se adapta a las necesidades de los usuarios.

proyecto de decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal y del Código Nacional de Procedimientos Penales en materia de delitos informáticos, evidencias digitales y medidas de cooperación internacional para combatir el ciberdelito, el cual fue publicado en la Gaceta Parlamentaria número 5013 del 26 de abril de 2018, particularmente en el Anexo XII de dicho órgano de difusión.

Dentro de este, incluye el delito de pornografía infantil a través de sistemas informáticos, la protección del derecho de propiedad intelectual para evitar la piratería informática, el acceso y alteración de la información o sistemas informáticos, de igual manera se reforman los artículos 211bis 1 a 211bis 7 que fueron adicionados al Código Penal Federal en 1999, además se adiciona un artículo 211 bis 8 que tipifica como delito la conducta de quien intercepte de forma dolosa y sin autorización por cualquier medio técnico, datos informáticos, información o comunicaciones dirigidas, originadas o efectuadas en o dentro de un sistema informático incluidas las emisiones electromagnéticas que transporten datos, información o comunicaciones, destaca por su importancia la propuesta de adicionar un capitulo III titulado como Delitos Informáticos y adicionan los artículos 211 Ter al 211 QUINTUS, tipificando como delitos a el abuso de dispositivos, la falsificación informática y la usurpación de identidad ajena; se adiciona al artículo 387 la fracción XXII para sancionar el perjuicio patrimonial por la introducción, alteración, borrado o supresión de datos informáticos.

Lo importante de este proyecto de dictamen es que se propone reformar y adicionar el Código Nacional de Procedimientos Penales, para que se tenga una sección titulada: “actos de investigación necesarios para la obtención de evidencias digitales”, adiciona los artículos 390 bis 1 al 390 bis 8 para establecer los procedimientos relativos a: Conservación de datos informáticos almacenados; Datos almacenados de usuarios o abonados; Registro y preservación de datos almacenados; Datos informáticos almacenados en otro Estado; Obtención de datos en

tiempo real; Cooperación y asistencia jurídica en materia procesal penal; Protección de datos personales en investigaciones.

Lo lamentable de este dictamen, es que no fue aceptado por las bancadas de los diversos partidos y se quedó en una mera propuesta de buenos deseos, por eso insistimos que es una reforma inconclusa.

La LXIV Legislatura federal no ha retomado esa interesante propuesta, solamente la Senadora Alejandra Lagunes Soto Ruíz, integrante del Grupo Parlamentario del Partido Verde Ecologista de México, presentó a la Asamblea una proposición con punto de acuerdo que exhorta al Ejecutivo Federal a iniciar, a través de un proceso de múltiples partes interesadas, los trabajos necesarios para la adhesión de México al Convenio sobre la Ciberdelincuencia, o Convenio de Budapest, lo cual requiere la invitación expresa del Comité de Ministros del Consejo Europeo ya que nuestro país no es miembro y tampoco participó en la negociación del Convenio.

El Plan Nacional de Desarrollo 2019 – 2024 del Presidente Andrés Manuel López Obrador, no contempla en ninguna de sus partes acción alguna en materia de ciberdelitos, por lo que consideramos recomendable:

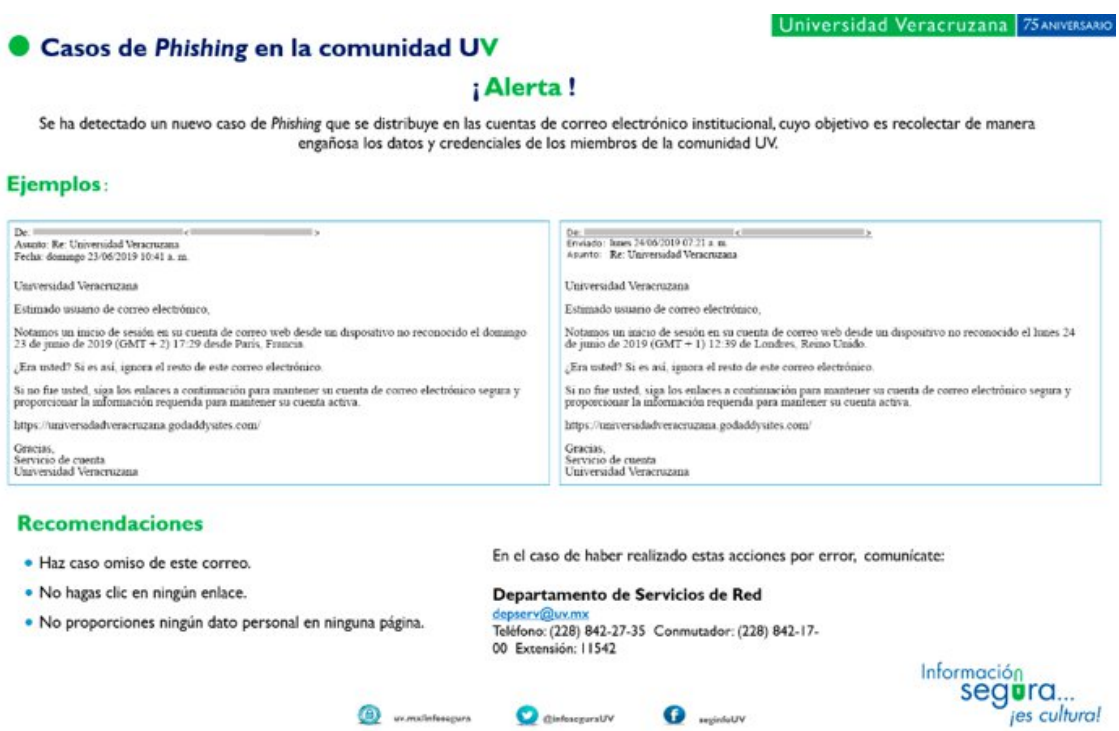
a) Que las universidades públicas y privadas contemplen en su Plan de Estudios como materia obligaría: “Derecho y las nuevas tecnologías de la información y comunicación”;
b) Impulsar acuerdos o convenios con los Gobiernos Federal, Estatal y municipal, para difundir y capacitar a sus trabajadores en esta nueva modalidad tecnológica;
c) Buscar mecanismos de coordinación con cámaras empresariales y legisladores federales para impulsar una nueva cultura en materia tecnológica y una nueva reforma legislativa más eficaz;
d) Constituir un grupo de especialistas para general una propuesta de reforma técnicamente viable, y
e) Fomentar los foros de discusión entre universidades de este tipo de temáticas.

Ejemplo caso de delito Cibernético.

En México las modalidades para cometer fraudes cuyo objetivo es el recolectar de manera engaños los datos y credenciales de los miembros de diferentes comunidades educativas y financieras han evolucionado e incrementado a lo largo de los años, lo que se ha visto reflejado en la cantidad de reclamos por parte de los usuarios que también ha ido en aumento.

Un ejemplo de delito cibernético es un nuevo caso de *phishing* en contra de los usuarios de la comunidad de la Universidad Veracruzana que a través de un correo electrónico, se notifica de un inicio de sesión de su cuenta de correo electrónico desde un dispositivo no reconocido, solicitando la verificación de identidad en un enlace externo en lo que este tipo de correos llevan al usuario a sitios falsos, donde solicitan datos que buscan obtener información personal y financiera para cometer fraudes.

Figura 1. Alerta de caso de phishing Universidad Veracruzana junio 2019.



Fuente: Universidad Veracruzana, 2019. En https://www.uv.mx/infosegura/files/2019/06/SGSI-Comunicados-CorreoNoUV_Junio2019.png

Conclusiones

La reforma al Código Penal Federal de 1999 para implementar los delitos informáticos en México, se encuentra rebasada por los avances tecnológicos y por la sofisticación de las conductas delictivas que existen en esta materia.

Europa y los organismos internacionales como la ONU y la UIT, han hecho estudios profundos sobre la ciberdelincuencia y su impacto en la sociedad, el gobierno y las empresas con sus respectivos efectos financieros, lo que ha generado en interesantes propuestas que los países desarrollados han adoptado y de los cuales nuestro gobierno no ha querido atender.

Los intentos legislativos para implementar reformas a la Ley Penal Federal y al Código Nacional de Procedimiento Penales, han sido insuficiente y socialmente han sido ignorados o desconocidos;

Urge una decidida participación de las Universidades para general cultura y propuestas objetivas y viables.

Bibliografía

Andrés Cámpoli, G. (2004). *Principios de Derecho Penal informático*. Ciudad de México: Ángel Editor.

Avast. (15 de mayo de 2019). *Cybercrime*. Obtenido de https://www.avast.com/es-es/c-cybercrime

Cisco. (2018). *Reporte Anual de Ciberseguridad*. San Jose, CA: Cisco Systems, Inc.

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2019). *Estadísticas*. Obtenido de https://www.condusef.gob.mx/gbmx/?p=estadisticas

Gobierno de los Estados Unidos Mexicanos. (2018). *6to Informe de Gobierno 2017-2018*. Ciudad de México: Presidencia de la República.

Nava Garcés, A. (2007). *Delitos Informáticos*. Ciudad de México: Porrúa.

Navarro Islas, J. (2005). *Delitos informáticos: México en el contexto mundial en Tecnologías de la Información y de las Comunicaciones: Aspectos legales*. Ciudad de México: Porrúa-ITAM.

Organización de las Naciones Unidas. (10 al 17 de abril de 2000). *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*. Obtenido de https://www.un.org/es/-conf/xcongreso/prensa/2088hs.shtml

Semanario Judicial de la Federación y su Gaceta. (2006). *Exacta aplicación de la ley penal.* La garantía, contenida en el tercer párrafo del artículo 14 de la constitución federal, también obliga al legislador. Ciudad de México: Poder Judicial de la Federación.

Téllez Valdés, J. (2009). *Derecho Informático*. Ciudad de México: Mc Graw Hill.

Villanueva, E. (2015). *Derecho de las nuevas tecnologías (en el siglo XX derecho informático.* Ciudad de México: Oxford.