

# La Cibercriminalidad y el Covid-19

Entrevista con el Dr. Alberto Nava Garcés

Investigador del INACIPE

Por Equipo Editorial

---

*Después de la pandemia no va a haber vuelta de hoja, los procesos se tendrán que llevar a cabo a través de las nuevas tecnologías, se tendrá que integrar a la vida cotidiana de la justicia.*

---

**A**ntes de la pandemia la Cibercriminalidad venía avanzando con tal velocidad que nos estaba rebasando en México y a nivel mundial, los códigos penales se quedaron rezagados, así como los cuerpos especiales de la policía cibernética. Por ejemplo, en 2018 y 2019 vivimos escandalosos hackeos y grandes fraudes a instituciones bancarias, hospitales e instituciones públicas, que quedaron en la impunidad absoluta. El surgimiento de la pandemia a principios de 2020 ha generado no solo una crisis de salud pública, económica y social, sino un alarmante auge de los ciberdelitos, con instrumentos delictivos novedosos como el phishing o el malware. Para hablar sobre este inquietante fenómeno, Foro Jurídico entrevistó al Doctor en Derecho Alberto Nava Garcés, destacado especialista en Derecho Penal, investigador y profesor del INACIPE y autor de varios libros sobre Cibercriminalidad. Presentamos a nuestros lectores la parte sustancial de la entrevista.

**FORO JURÍDICO (FJ): ¿QUÉ NOS PODRÍA COMENTAR SOBRE LA CIBERCRIMINALIDAD Y LA PANDEMIA?**

**ALBERTO NAVA GARCÉS (ANG):** Mi primera reflexión sería que si esta pandemia nos hubiera tocado hace 25 años, nos hubiera mandado al medioevo inmediatamente. Estaríamos desconectados, no contaríamos con tantos servicios sin tener que salir de casa, como los tenemos en la actualidad.

Las tecnologías no han sido utilizadas al 100%, pero han servido para salvar los tiempos difíciles en los que vivimos. Sin embargo, el hecho de hacer tanto uso de la tecnología no nos deja exentos de posibles delitos que se cometen a través de estos medios. Si todos estamos sujetos a un encierro, la delincuencia también está sujeta a estas nuevas reglas. Ahora que nos hemos vuelto dependientes de las tecnologías para obtener servicios, nos hemos dado cuenta de que la delincuencia también ha migrado a ese tipo de nichos. Estos delitos son diversos, desde personas que lucran vendiendo productos para preservar la salud (medicinas falsas, oxígeno, vacunas, etc.) hasta quienes ofrecen distintos productos falsos de entretenimiento. Es decir, los fraudes abarcan desde servicios simples hasta graves.

**FJ: CON ESTA CLASIFICACIÓN DE SIMPLE Y GRAVE, ¿PODRÍAMOS CONSIDERAR COMO UNA NUEVA MODALIDAD DE CIBERDELITO LA VENTA DE OXÍGENO PORQUE ESTÁN LUCRANDO CON EL DOLOR DE LA GENTE?**

**ANG:** El propio titular de la Profeco hizo una mención al oxígeno que se estaba ofertando y en cierto modo ese oxígeno de uso industrial sirve para encender un soplete y no para salvar a un enfermo. Hay que tener cuidado de que el oxígeno sea para uso médico y no industrial. El hilo conductor de la delincuencia en estas situaciones es la ingeniería social que aplica en su tratamiento. Se trata de explotar las necesidades urgentes de la población, Entonces entra la ingeniería social a vender productos que explotan nuestras preocupaciones.

La ingeniería social ocurre desde antes de las tecnologías, pero las tecnologías permiten que ésta sea explotada de manera exponencial. La ingeniería social se encarga de detectar qué es lo que busca el mercado y cuáles son sus preocupaciones, a partir de esto empieza a vender productos o servicios falsos a través de los cuales la delincuencia obtiene ingentes ganancias. Como dicen los italianos, los delincuentes les ponen la pulga en la oreja a los consumidores, explotan su preocupación, estas personas prácticamente buscan al delincuente en los sitios equivocados.

**FJ: UN RECIENTE REPORTE DE LA INTERPOL**



**SEÑALA QUE LOS CIBERDELICUENTES HAN PASADO DE HACKEAR A PARTICULARES A DEFRAUDAR GRANDES EMPRESAS. QUE EN LA PANDEMIA HAN ATACADO BASES DE DATOS DE HOSPITALES PARA EXTRAER INVESTIGACIONES SOBRE EL COVID-19 Y MUCHOS ESTADOS SE HAN QUEDADO CON POCOS RECURSOS PARA COMBATIR ESTOS DELITOS. ¿QUÉ OPINA AL RESPECTO?**

**ANG:** No hay que confiarse demasiado en que los hackers se enfocan en ataques a las grandes empresas y en los

*“Es importante señalar que las personas tienen corresponsabilidad en el tipo de operaciones y en el uso que hacen de su tarjeta. Si se mete a distintos lugares sin verificar la seguridad de las páginas y proporciona los datos de su tarjeta de bancaria y de usuario, de alguna manera aumenta potencialmente el riesgo.”*

Estados, porque el encierro nos obliga a utilizar recursos virtuales, tarjetas bancarias, información personal, ese es el foco en el que se concentran los ciberdelincuentes para tener grandes ingresos. El año pasado, a inicios de la pandemia, la Interpol ya había publicado un documento donde exponía ese tipo de alertas. La primera recomendación es no tenerle miedo a las nuevas tecnologías, sino utilizarlas con sentido común. Se debe ir a sitios seguros para realizar este tipo de operaciones.

En esta pandemia hemos proporcionado más veces nuestros datos personales que en toda nuestra historia, y esto ocurre sobre el teletrabajo, el cual es parte de las soluciones al distanciamiento social que guardamos y que hace pocos días tuvo que ser materia de una reforma porque de alguna manera cada vez estamos más involucrados en este tipo de procesos en los cuales entregamos nuestro trabajo, pero también existen páginas que ofrecen trabajos falsos de teletrabajo donde las personas terminan siendo el objeto para engañar a otras sobre alguna oferta de trabajo.

Esta situación forma parte de la explotación de las preocupaciones y necesidades que tenemos que enfrentar. Otra modalidad más grave es la explotación de los sentimientos solidarios, en los cuales exponen casos falsos de Covid-19 para pedir apoyo económico y cubrir los supuestos tratamientos a través de transferencia o de proporcionar los datos de tarjetas bancarias.

**FJ: ¿CÓMO HAN RESPONDIDO LAS**

### **CIBERPOLICÍAS A ESTE FENÓMENO?**

**ANG:** Comencemos por recordar cómo enfrentamos la pandemia cuando apareció: con miedo. En un primer momento sin saber cuáles son sus alcances, cuál su potencial, la mortandad y demás datos. Todos tuvimos miedo por no saber cómo enfrentar este tipo de cuestiones. El aprendizaje ha sido doloroso, porque a pesar de que ya contábamos con algunos procesos automatizados, por ejemplo, la Ley de Amparo de 2013 ya preveía el procedimiento electrónico en materia administrativa, prácticamente ya estaba todo el procedimiento encaminado.

En muchas materias, familiar, la violencia intrafamiliar se incrementó, en este caso el gran problema fue cómo le hacemos si tenemos una Procuraduría o Fiscalía cerrada, porque hay muchos contagios, porque no se sabe qué tan fuerte puede ser esta ola de contagios, y así vemos que las autoridades se quedaron a mitad del camino, semiparalizadas. Salían acuerdos para suspender actividades, para postergar muchas de las cuestiones judiciales de índole penal. Aparecieron anuncios de fiscalías que iban a trabajar en la modalidad de home office porque no podían atender presencialmente por el alto nivel de contagios. Es decir, la atención policiaca en la materia ha sido deficiente.

Como ya lo afirmé, la experiencia ha sido dolorosa, pero después de la pandemia no va a haber vuelta de hoja, los procesos se tendrán que llevar a cabo a través de las nuevas tecnologías, se tendrá

que integrar a la vida cotidiana de la justicia. A pesar de que ya era una realidad, todo mundo lo tomaba como algo de ciencia ficción, pensaban que no era una cuestión de recursos, ahora lo es, en donde podremos ver a los magistrados sesionando a través de dispositivos. El aprendizaje ha sido duro, pero los resultados a mediano plazo serán positivos.

### **FJ: ¿POR QUÉ CONSIDERA QUE NO DEBEN SER TRATADOS DE LA MISMA MANERA, MINISTERIAL Y JUDICIALMENTE LOS DELITOS TRADICIONALES Y LOS CIBERDELITOS?**

**ANG:** En el terreno de los delitos informáticos propiamente dichos, hace 20 años eran considerados delitos tradicionales cometidos mediante métodos electrónicos. Poco a poco los delitos fueron migrando y tomaron identidad propia, al grado de que la información como tal se convirtió en el objeto del delito. De pronto la identidad electrónica de la persona para su uso en redes se convirtió en una cuestión específica, esto fue lo que abrió la brecha entre los delitos tradicionales y los informáticos.

En lo referente a la justicia electrónica, tenemos que tomar en cuenta que cuando se resolvió el primer divorcio en la Ciudad de México por medios electrónicos, fue celebrado con demasiado optimismo.

Es curioso este tipo de cuestiones porque establecían cómo tenía que ser la justicia, cómo aprender a identificar a las partes, ratificar la identidad de la persona que está del otro lado de la pantalla, acreditar sus personalidades.



*“La violencia digital es un fenómeno reciente que nace con la tecnología, con situaciones que ocurrían anteriormente, pero que se adaptaron a la nueva realidad. Cuando Olimpia Coral acudió al Ministerio Público por primera vez a denunciar que su expareja subió videos de índole sexual a internet, el MP no supo cómo encuadrar la denuncia, no podía encasillarlo dentro de un tipo penal.”*

Mientras nosotros echábamos la casa por la ventana para celebrar estos avances, en Colombia y en España estaban echando abajo algunas sentencias que se habían dictado para juicios que habían ocurrido a través de medios electrónicos. Tenemos que aprender a adaptar nuestra justicia a esta clase de medios, es una cuestión de nuevo aprendizaje.

#### **FJ: ¿QUÉ DEBEMOS HACER CUANDO NOS HACKEAN UNA CUENTA DE BANCO?**

**ANG:** Los bancos ponen algunas medidas de seguridad para que las personas puedan realizar operaciones electrónicas. También los bancos se han ido adecuando a esta nueva modalidad digital. Han ido proporcionando

plataformas más amigables para poder realizar transacciones. Existen empresas que permiten realizar transacciones de manera segura, por ejemplo, Pay Pal, que sirven como escudo entre la transacción y la tarjeta bancaria, de modo que el recurso económico se libera hasta que el comprador recibe el producto, lo cual garantiza la transacción y la calidad del producto recibido. El problema es que hay pocos intermediarios como Pay Pal. Algunos bancos han querido hacer ese tipo de operaciones proporcionando un número de operación variable para que solamente funcione en una transacción y evitar el fraude.

Cuando ya tenemos el problema encima, en primer lugar, debemos avisar al banco para que bloquee la cuenta. No hay

otro mecanismo de carácter inmediato para evitar mayores transacciones. El banco sabe que va a tener que enfrentar un proceso de reclamación para que de manera inmediata detecte cómo fue utilizada, cuál fue el patrón, hacia dónde fueron los recursos para saber si se puede cancelar la operación y saber si opera el seguro que tienen los cuentahabientes. Mientras que el afectado debe acudir al ministerio público para denunciar el robo de recursos.

Es importante señalar que las personas tienen corresponsabilidad en el tipo de operaciones y en el uso que

*“La tecnología siempre va a estar un paso adelante del Derecho porque evoluciona de una manera galopante, la única manera de contrarrestar este tipo de acciones es que la tecnología se vence con tecnología, después vendrán la tipificación, los delitos y lo demás.”*

hacen de su tarjeta. Si se mete a distintos lugares sin verificar la seguridad de las páginas y proporciona los datos de su tarjeta de bancaria y de usuario, de alguna manera aumenta potencialmente el riesgo. La responsabilidad está en el banco en tanto la operación sea detectada a tiempo, hay muchos casos de éxito en donde el banco le restituye el dinero al afectado.

También debemos tomar en cuenta que son dos escenarios distintos los que pueden ocurrir con los asuntos bancarios: no es lo mismo que saqueen la tarjeta de crédito, porque finalmente el dinero que roban no es el del afectado, sino del banco, a que saqueen la tarjeta de débito, en la cual la persona guarda sus propios recursos; por lo cual se debe aprender qué tarjeta usar para este tipo de transacciones.

**FJ: CON LA PANDEMIA TIENES QUE CONTRATAR REITERADAMENTE SERVICIOS Y DAR FRECUENTEMENTE LOS DATOS DE TU TARJETA**

**DE CRÉDITO, LO QUE AUMENTA EL RIEGO DE QUE TE COMETAN CIBERDELITOS. ¿COMO PREVENIRLOS?**

**ANG:** Como ocurre con las personas en la vida real, las plataformas van ganado reputación por el cuidado que tienen en el tratamiento de datos. Por esta razón podemos pedir los productos a determinadas plataformas que garantizan la seguridad de nuestros datos sin temor a ser defraudado. Existe una Ley de protección de datos en Posesión de los particulares, que hace que las plataformas tengan que responder ante el INAI, un organismo que ahora quieren desaparecer, pero hay que tener una visión amplia sobre qué funciones cumplen los órganos, en este caso el propio INAI, porque son validadores de las plataformas y del uso que hacen de nuestros datos.

**FJ: ¿EXISTE ALGÚN CONVENIO INTERNACIONAL QUE REGULE LOS CIBERDELITOS?**

**ANG:** Después de los ataques a las Torres Gemelas en 2001, Estados Unidos le dio una mayor importancia al tema de la ciberdelincuencia, porque varias de las actividades que realizaron los terroristas fueron a través de la red. La presión de EE. UU. fue tal que en Europa se estaba redactando un documento para crear el Convenio de Cibercriminalidad de Budapest, que se firma en noviembre de 2001. Sin embargo, ni EE. UU. ni México lo firmaron. Durante varios años han prometido firmarlo, se convirtieron en observadores, pero nunca ha sucedido.

Cuando México firme dicho Convenio, será obsoleto porque es de 2001 y el auge de los cambios tecnológicos es más reciente, es decir se ha perdido la vigencia del Convenio de Cibercriminalidad. México retrasó la firma porque tenía que adaptar sus leyes. En la práctica ya ha ido adaptando tipos penales y procedimientos relacionados con aspectos tecnológicos.

**FJ: LA RECIENTE APROBACIÓN DE LA LEY OLIMPIA, QUE SANCIONA LA VIOLENCIA DIGITAL, SURGE DE LA EXPERIENCIA QUE VIVIÓ EN CARNE PROPIA LA JOVEN OLIMPIA CORAL MELO ¿QUÉ OPINA AL RESPECTO?**

**ANG:** La violencia digital es un fenómeno reciente que nace con la tecnología, con situaciones que ocurrían anteriormente, pero que se adaptaron a la nueva realidad. Cuando Olimpia Coral acudió al Ministerio Público por primera vez a denunciar que su expareja subió videos de índole sexual a internet, el MP no supo cómo encuadrar la denuncia, si considerarlo abuso, acoso, no podía encasillarlo dentro de un tipo penal. Lo único que consiguió Coral fue ser revictimizada, pero con el carácter resiliente que mantuvo logró extraer de su mala experiencia un proyecto de ley. Actualmente, los jóvenes, casi niños, deben enfrentarse a este tipo de problemas, ya que tienen la costumbre de compartir entre ellos el pack, un portafolio de imágenes íntimas que es subido a las redes sociales. Con el alcance del internet la difusión es exponencial.

Muchas veces no se calcula en daño que puede llegar a causar este tipo de violencia en la autoestima de la persona agredida. En este sentido, Olimpia Coral consiguió que la pornovenganza, la violencia digital, todo lo relacionado con la exposición de la persona a nivel digital, se tipifique finalmente como un delito. Fue bastante exitosa la gestión de Olimpia ya que varias legislaciones han ido adaptando la Ley Olimpia de manera paulatina a sus propios códigos.

### FJ: TOMANDO EN CONSIDERACIÓN QUE LOS CIBERDELITOS SE REALIZAN A TRAVÉS DE MEDIOS TECNOLÓGICOS, CON UN SUPUESTO CONOCIMIENTO ESPECIALIZADO DE MECANISMOS SOFISTICADOS, ¿SON DELITOS AGRAVADOS?

ANG: Agradecería con que el propio delito informático estuviera tipificado porque el gran problema es que no aparecen en muchas legislaciones. No podemos dar el segundo paso cuando no se ha dado ni siquiera el primero que es legislarlo. En materia de tecnología tenemos que recordar un principio ante de la propia tipificación: la tecnología siempre va a estar un paso adelante del Derecho porque evoluciona de una manera galopante, la única manera de contrarrestar este tipo de acciones es que la tecnología se vence con tecnología, después vendrán la tipificación, los delitos y lo demás. Mientras los abogados prometamos únicamente una legislación y el problema de hackeos, robo de identidad, sabotajes a nivel electrónico,

etcétera, no sean prevenidos con tecnología, ninguna legislación puede ser efectiva, sobre todo porque vivimos en una época en la que estando todos encerrados somos más vulnerables a este tipo de ataques. Tenemos que aprender a ser cautos utilizando el sentido común, no esperar a que el derecho penal o las propias autoridades puedan responder a esta masificación de delitos.

Una de las cosas más interesantes que vienen en

materia de justicia cotidiana penal es que actualmente tanto la Fiscalía de la República como la de la Ciudad de México están reordenando sus estructuras, Tendrán que valorar el delito informático que está cometándose de manera más recurrente.

El delito informático tiene una base de ingeniería tecnológica, por lo cual las autoridades necesitarán de equipos técnicos y de abogados que estén a la altura de este problema. 

