CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS, A.C.

FALSOS PORTALES QUE CONECTAN A MÉXICO CON EL CIBERCRIMEN TRANSNACIONAL

CIBERDELINCUENTES YA NO ASALTAN BANCOS NI CASAS; CON INTERNET Y UN CLIC ATACAN A SUS VÍCTIMAS, ESTA AMENAZA PARA LOS CIBERNAUTAS APENAS EMPIEZA.

TESIS

QUE PARA OBTENER EL GRADO DE

MAESTRA EN PERIODISMO SOBRE POLÍTICAS PÚBLICAS

PRESENTA:

ANA LAURA VÁSQUEZ SARMIENTO

DIRECTORA DE TESIS:

DRA. MARÍA SOLANGE MAQUEO RAMÍREZ

LECTOR DE TESIS:

MTRO. CARLOS PUIG

CIUDAD DE MÉXICO

JUNIO, 2019

"…Para el periodismo de investigación no resulta fácil prosperar en una cultura predominantemente oral. Los números, las cifras, las estadísticas no son tan apreciadas como las palabras, el ritmo y la estructura. Afortunadamente este hecho no necesariamente obstaculiza el trabajo: al contrario, el periodista que domina sus herramientas puede transformarlo en una enorme ventaja.

El verdadero problema estriba en la comprensión (o incomprensión) general de nuestras sociedades acerca de qué es el periodismo de investigación. Debemos seguir educando para que el público en general esté de nuestro lado, de lo contrario siempre será bastante fácil acusar al periodista de ser un espía cuando este investiga.

No hace falta decir que esta forma avanzada de periodismo conlleva, además, riesgos de tipo mental, emocional, psicológico y social. (…) A cambio sentirán la felicidad de encontrar hilos conductores y de atar cabos; y el placer máximo e indescriptible de hacer un descubrimiento.

Pero, sobre todo, no hay nada como el sentimiento terapéutico que se tiene cuando alguien que no debía saber nada se te acerca y te dice "muchas gracias", "felicidades", "muy buena nota". Ese gesto bastará para lanzarte a perseguir una nueva historia…"

Extracto del Prefacio escrito por Yosri Fouda, Corresponsal Jefe de Investigación de Al Jazeera, en el libro *La investigación a partir de historias: Manual para periodistas de investigación.* Mark Lee Hunter.

Gracias

Gracias, a la Fundación Legorreta Hernández y a su presidente Alejandro Legorreta, por creer en el periodismo, por creer en los periodistas, por creer en mí y ayudarme con la Beca Legorreta Hernández a hacer realidad uno de mis sueños. Los periodistas también contribuimos al desarrollo social en México y volvemos parte de nuestras circunstancias las condiciones en las que viven millones de mexicanos, así que "hagamos lo que nos toca siempre con esperanza".

Redactar no es todo lo que se requiere para hacer periodismo; cada letra, cada párrafo, cada texto, en mi opinión, tienen que remover sentimientos, generar ideas, incitar la reflexión, impulsar el cambio para bien; lograrlo demanda de maestría. Gracias a las víctimas del fraude cibernético por su testimonio, especial dedicatoria y reconocimiento les expreso en estas líneas, así como mi deseo de que algún día reciban justicia.

Angulos nuevos del periodismo, estrategias para encontrar fuentes, técnicas de narrativa, entre otras enseñanzas para construir una pieza periodística es lo que me llevo de cada uno de mis maestros. Gracias a todos por compartir conmigo sus conocimientos y experiencia. Me toca a mí perfeccionar las lecciones aprendidas y aprehendidas.

Citar en estas líneas cada una de las enseñanzas que recibí durante mi estancia en el CIDE quisiera, pero este espacio no me alcanzaría. Gracias por contagiarme de la emoción de aprender cada día y también de enseñar a otros lo aprendido.

Imagino ahora un nuevo camino para mí en el periodismo, más estilizado, más refinado, más inteligente, de mayor conocimiento y trascendencia, pero sobre todo más valorado. Que se haga realidad mi imaginación.

Agradecer es la semilla de la abundancia, del crecimiento, florecimiento y maduración de nuevos frutos. Agradezco a mi familia por entender mi ausencia para alcanzar esta meta de mi proyecto de vida, me era ineludible agregar a él nuevas lecciones.

Sin duda esta es una nueva sección de mi historia profesional y personal por la que debo dar gracias porque el agradecer también es un ingrediente para atraer lo positivo de la vida.

Ana

Índice

Falsos portales que conectan a México con el cibercrimen transnacional

Ciberdelincuentes ya no asaltan bancos ni casas; con internet y un clic atacan a sus víctimas, esta amenaza para los cibernautas apenas empieza.

Por Ana Laura Vásquez Sarmiento

Espacio físico y ciberespacio

Internet no es un mundo paralelo al espacio físico en el que vivimos, no existe tal separación, porque quienes caminan por las calles, quienes conversan en la sala de casa, quienes ven el noticiario a través de la televisión, Facebook, YouTube o hacen compras desde la página electrónica de una reconocida cadena comercial y también los delincuentes son los mismos que utilizan, alimentan y dan vida a Internet.

Todos ellos están ahí, en el espacio físico y también en el *ciberespacio*[1] materializado por las redes y sistemas que permiten la comunicación entre computadoras y personas. El Internet existe porque los humanos lo crean, y se transforma y propaga mientras lo usan.

"Conforme Internet se vuelve más potente y su uso se expande a cada vez más lugares, personas y condiciones, se convierte en un espejo más fiel de la humanidad, y con ello también sirve para expresar malas intenciones y para hacer daño real a las personas".[2]

Ese daño real, insertado del espacio físico al ciberespacio, alcanzó a David, Rosa, Norberto, Escribano, Isaac, Edgar y Jesús. Ellos no se conocen, ninguno sabe de la existencia del otro, aun así, las historias de cada uno se entrelazan en Internet y tienen algo en común; los siete vivieron

[1] El término *ciberespacio* hace referencia al conjunto de redes y sistemas que habilita la comunicación entre computadoras, personas y otros dispositivos. Dicha comunicación permite transmitir correos electrónicos, consultar páginas web, utilizar servicios digitales y realizar transferencias económicas, entre muchas otras actividades. El ciberespacio no es un sinónimo para la internet, más bien la internet es un "subconjunto" del ciberespacio. (Rodrigo Riquelme 2019-*El Economista*).

[2] Pisanty A. *Llámame Internet*. Caja Chica-Secretaría de Cultura. Junio 2018. Pág., 20.

la misma experiencia al caer en un fraude operado con Internet y planeado por seres humanos como ellos, pero con malas intenciones.

Ciberdelincuentes, como ahora les llaman, clonan portales electrónicos con la imagen corporativa de reconocidas empresas y ofertan desde ahí flotillas de automóviles en remate supuestamente propiedad de grandes corporaciones tanto públicas como privadas, que usan como gancho para atraer víctimas y defraudarlas con miles de pesos. Es una modalidad de fraude cibernético transnacional operado con Internet en el ciberespacio.

El sueño de comprarse un automóvil llevó a David, Rosa, Norberto, Escribano, Edgar, Isaac y Jesús a caer en ese tipo de fraude cibernético. En el ciberespacio se encontraron con un remate de flotillas que supuestas reconocidas empresas ofrecían a través de los portales electrónicos, y sin haber visto físicamente los vehículos pagaron por ellos y nunca los recibieron.

No son ingenuos, tampoco incautos; simplemente son víctimas de un delito consumado por delincuentes que aprovechan Internet para delinquir porque los beneficia con el anonimato y la impunidad, amplifica su impacto, el delito ocurre con mayor velocidad y reduce costos.

Esta realidad refleja la vulnerabilidad de los usuarios de internet en el ciberespacio porque si bien en México existe una estrategia de ciberseguridad ésta aparentemente no es efectiva. Los ciberdelincuentes operan con impunidad y los cibernautas son víctimas del crimen cibernético.

El modelo delictivo en el ciberespacio parece idéntico al que ocurre en el espacio físico, pero no lo es, la diferencia es que con Internet se complejizan o incrementan los problemas jurídicos; por ejemplo, la ubicuidad de Internet puede deslocalizar[3] al victimario, le permite instalarse en otro país y hace que su localización sea distinta a la de la víctima, lo cual excede la capacidad de las autoridades nacionales que corresponden al lugar de la comisión del delito para procurar y administrar justicia. Los conflictos de jurisdicción y el alcance de las autoridades competentes hacen del hecho delictivo un asunto globalizado de difícil resolución.

Internet es barato, rápido y altamente rentable para delinquir. Cuesta apenas mil pesos, o poco más, un dominio y un *hosting* para instalar en el ciberespacio una página electrónica ficticia y operar desde ahí un fraude cibernético transnacional.

[3] La deslocalización es el traslado a otro país y la nueva instalación en el lugar elegido.

En ocasiones, ni siquiera es necesario pagar porque con habilidades y herramientas digitales es posible vulnerar un servidor ajeno e insertar un portal electrónico utilizado para el delito; o sencillamente aprovechar a los intermediarios de Internet que ofrecen una página web gratuita. Una vez creado el sitio electrónico ficticio se puede promocionar en MercadoLibre, otros mercados electrónicos o, incluso, en redes sociales como Facebook, donde el costo no rebasa los 300 pesos.

Los ciberdelincuentes son expertos en violar cualquier esquema de seguridad en el ciberespacio así sea de los más avanzados, aunque no siempre se valen de esas herramientas; también recurren a la manipulación y engaño de sus víctimas, una técnica científicamente conocida como *ingeniería social* con la que inducen a su víctima a que haga algo, diga algo o deje de hacer algo que a ellos les va a beneficiar. No vulneran ningún sistema computarizado, simplemente maniobran con la mente humana.

Las posibilidades de que los ciberdelincuentes sean sorprendidos y capturados son prácticamente nulas. En México, de 2014 a enero de 2019, al menos 526 personas físicas y morales fueron víctimas del fraude cibernético a través del falso remate de flotillas; y aunque todos denunciaron, las procuradurías y fiscalías locales del país no reportan a ningún detenido.

Un cumpleaños inolvidable y un fraude transnacional

Este no es un día normal para Jesús, es especial porque celebra su cumpleaños y como es su costumbre, cada año, él mismo se consiente por la ocasión. Además de usar ropa elegante y arreglarse mejor que todos los días, tiene en sus planes comprar un auto. Ese será su regalo.

Son las 09:00 horas del 11 de marzo de 2015, relata que a esa hora y ese día, una vez que se había arreglado tomó su teléfono celular y llamó a la agencia de autos donde ya hacía los trámites para comprar una camioneta seminueva, pero la asesora automotriz le responde que los 100 mil pesos que él tiene disponibles no son suficientes para dar el enganche de la unidad incluida en el catálogo de los seminuevos y que además otro cliente ya dio el apartado por la camioneta que él quería.

En ese momento, en la pantalla de su computadora estaba abierta la página del portal electrónico MercadoLibre que visitaba desde días anteriores para buscar un automóvil, y justo exhibía una oferta: "Por renovación de parque vehicular Cementos Cruz Azul remata sus flotillas, para más información haga clic en la siguiente liga". La publicación vinculó a Jesús, desde MercadoLibre con la página *web* www.cementelca.com donde había un catálogo digital de automóviles, camionetas tipo SUV, unidades de carga y maquinaria pesada.

Automóviles Corsa a la venta en 40 mil pesos; camionetas de carga en 100 mil pesos; una CRV de Honda, por 140 mil pesos; y la que a él le llamó la atención, una camioneta Mazda CX5 2015 en oferta por 112 mil pesos. Era un supuesto remate de flotillas corporativas de la cementera.

La suerte parece estar de su lado, el cumpleañero está seguro de que tendrá su regalo; la camioneta que él quiere cuesta en el mercado al menos 300 mil pesos y él la encontró en una ganga. Feliz cumpleaños, piensa.

Ese regalo, en realidad lo llevó a perder su dinero y tranquilidad, y lo que él imaginó para celebrar su cumpleaños se convirtió en una pesadilla. Jesús cayó en un fraude[4] operado con

[4] El Código Penal Federal de México (CPF) describe en su artículo 386 que "comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido". En el entendido que la conducta ilícita está tipificada, debe considerarse por fraude cibernético el delito que se comete y desarrolla con las mismas características, pero con Internet o el uso de medios informáticos y dispositivos electrónicos.

Internet por el que los defraudadores usaron como gancho un remate falso de flotillas exhibido en portales electrónicos ficticios con la imagen corporativa de reconocidas empresas.

Se trata de un fraude cibernético[5] transnacional[6] porque ocurrió en México, pero el dinero de Jesús ingresó a las ganancias de casinos en Lima, Perú, como si un jugador lo hubiera gastado en las casas de juegos. No es un caso aislado; se pudo documentar la misma estafa en agravio de otras cuatro víctimas, David, Escribano, Isaac y Edgar, consumada con igual estrategia delictiva y la misma ruta para el dinero de México a Perú.

Cinco de los casos de los que se tiene testimonio y evidencia sucedieron a principios de 2015; en noviembre de ese año Rosa también cayó en la estafa; y en 2017, Norberto vivió la misma experiencia, aunque ellos dos desconocen el destino de su dinero. Para 2019 los siete agraviados todavía esperan justicia porque las autoridades no han resuelto sus casos, mientras esta modalidad de fraude cibernético sigue vigente como lo evidencia un monitoreo a mercados electrónicos.

Ciberdelincuentes captan víctimas con anuncios clasificados en MercadoLibre, SegundaMano, OLX, VivaAnuncios, Venderbien, etc., también usan falsos perfiles empresariales en la red social de Facebook desde donde vinculan a los cibernautas con sitios electrónicos falsos.

El monitoreo detectó portales electrónicos clonados de las empresas Cementos Cruz Azul, Bimbo, Grupo México, Femsa, Herdez, Ford, Coca Cola, Cemex, Grupo Modelo, Barcel, Bonafont, Minera Frisco, Soriana, Gamesa, Volaris y otras; así como de Petróleos Mexicanos (Pemex), Secretaría de Comunicaciones y Transportes (SCT), Secretaría de Hacienda y Crédito Público (SHCP), Comisión Federal de Electricidad (CFE), Fondo Nacional de Turismo

[5] El Convenio de Budapest, en su artículo 8 relativo al fraude cibernético, tipifica este delito como los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos; asimismo, cualquier interferencia en el funcionamiento de un sistema informático con la intensión, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

[6] La Organización de las Naciones Unidas (ONU) define los delitos transnacionales como aquellos cuya iniciación, prevención y efectos directos o indirectos afectan a más de un país. En 1995 consideró 18 categorías de criminalidad transnacional: lavado de dinero, actividades terroristas, robo de arte y cultura, tráfico de armas, robo de propiedad intelectual, secuestro de aviones, piratería marítima, corrupción y soborno de funcionarios públicos o partidistas, fraude de seguros, delitos ambientales, tráfico de órganos, narcotráfico, quiebra fraudulenta, infiltración de negocios legales, tráfico de personas, crimen informático.

(Fonatur) y la extinta Secretaría de Agricultura Ganadería Pesca y Alimentación (Sagarpa), todos utilizados para rematar o subastar falsas flotillas, unidades de carga y maquinaria pesada.

Además, ubicó 20 líneas telefónicas contratadas a Megacable y Telcel, según el registro del Instituto Federal de Telecomunicaciones (IFT), usadas como canal de comunicación con las supuestas empresas, pero en realidad es el contacto entre los defraudadores y las víctimas.

La historia de Jesús como la de David, Rosa, Escribano, Isaac, Norberto y Edgar, refleja lo fácil y barato que es habilitar en el ciberespacio decenas de páginas electrónicas y con la velocidad del Internet ganar en unos minutos u horas miles de pesos a través del fraude.

“Todo es muy barato, por un año puedes comprar dominios hasta en seis dólares; tener una página (electrónica) te puede costar diez dólares, o sea, no es una inversión tan grande comparado con lo que obtienen por el enganche o apartado del auto. La rentabilidad es muy alta”, explica Andrés Velázquez, fundador del primer laboratorio de investigación de delitos informáticos en América Latina.

Delinquir desde el ciberespacio es rápido, altamente rentable y con garantía para los ciberdelincuentes de no ser atrapados. Por este tipo de fraude cibernético no hay ningún detenido y menos algún sentenciado en el país, de acuerdo con información que proporcionaron las procuradurías y fiscalías locales.

Jesús recuerda que ese día de su cumpleaños, se sentía emocionado por consentirse él mismo y tener la capacidad económica para comprarse un automóvil como regalo. Al ver la tentadora oferta, llamó al teléfono de contacto para solicitar información; le contestaron tal cual una llamada a una consolidada y seria compañía.

“Cementos Cruz Azul, buenos días”, dijo un varón en el altavoz, quien, al escuchar a Jesús interesado por comprar una camioneta, lo transfirió al área de ventas.

Mientras esperaba en el teléfono, relata que se persignó ante una imagen de la virgen de Guadalupe que cuelga de la pared pegada a la cabecera de su cama y le rogó que todo saliera bien.

En el teléfono, Carlos Lozada Martínez se presentó como Gerente de Ventas de Cementos Cruz Azul, le informó el proceso de compraventa y el método de pago que Jesús aceptó emocionado.

Cerrado el trato, Lozada Martínez ofreció enviarle por correo electrónico un contrato de compra venta y después de que lo firmara y regresara por el mismo medio junto con una identificación oficial y comprobante de domicilio, debía confirmar un depósito del 50 por ciento o el total, ya fuera directamente en caja o por transferencia electrónica SPEI para que se reflejara el mismo día a una cuenta bancaria en Banorte, a nombre de Ana Castillo Gómez, quien dijo era la representante legal de la cementera.

Hasta verse reflejado el depósito, la camioneta saldría hacia su domicilio desde Veracruz a la ciudad de Puebla**,** junto con dos juegos de llaves, los documentos que acreditaban que no tenía reporte de robo, las tenencias y verificaciones, así como el chofer que la llevaría y a quien debía acercar a una terminal camionera para su regreso, una vez que la entregara.

Jesús fue al banco y depositó los 112 mil pesos para pagar la camioneta, a las 10:59 horas de ese día de marzo de 2015, en una sucursal de Banorte, a favor de Castillo Gómez, según lo detalla el estado de la cuenta bancaria certificado por la Comisión Nacional Bancaria y de Valores (CNBV), obtenido para esta investigación.

La víctima narra que le informó a la cajera del banco que se trataba de un depósito para Cementos Cruz Azul y que ésta lo miró con las cejas fruncidas, como cuando alguien se extraña de algo.

Al salir de la sucursal bancaria recibió en su teléfono celular una llamada de Lozada Martínez, quien le confirmó que ya estaba el dinero en la cuenta y que el chofer iba en camino con la camioneta monitoreado con un censor de velocidad.

A las 17:00 horas, a más tardar, el chofer llegaría con la camioneta para entregarla en su domicilio, pero dieron las 18:00 y 19:00 horas; nadie llamó a la puerta.

Cuando el reloj marcó las 20:00 horas, Jesús empezaba a reaccionar y a asimilar que el remate de flotillas era un engaño.

“Todo parecía tan formal, serio, pues era Cementos Cruz Azul, me dieron informes por la camioneta y yo ofrecí el dinero, le dije al gerente de ventas que yo iría por ella o que tenía la posibilidad de mandar a un amigo de mi confianza que es policía para que la recogiera, pero me dijo que era una empresa seria y que con toda seguridad me podían mandar la camioneta a mi domicilio. Nunca me llegó”, cuenta.

De la emoción Jesús pasó a la frustración, recuerda que su cuerpo empezó a temblar cuando en su reloj dieron las 20:00 horas y nadie tocó la puerta de su casa para entregar la camioneta que sería su regalo de cumpleaños.

Dice que hizo hasta 20 llamadas a las oficinas de Cementos Cruz Azul, pero nadie respondió; decidió ir a dormir con la esperanza de que algún incidente hubiera ocurrido y al amanecer tendría buenas noticias.

Al día siguiente despertó con la sensación de haber tenido una pesadilla. Esperó a que dieran las nueve de la mañana, normalmente el inicio de un horario laboral, para volver a marcar a la oficina de Cementos Cruz Azul. Sus llamadas ya no entraban, solo se escuchaba un tono extraño que interrumpía la marcación. Su intuición ya le indicaba algo irregular en la compra-venta que había concretado el día de su onomástico.

Entonces tuvo la idea de marcar desde un teléfono diferente al que utilizó en principio y hacerse pasar como un nuevo cliente interesado en el remate de las flotillas de Cementos Cruz Azul.

Ocurrió el mismo proceso, le contestó un recepcionista, lo transfirió al área de ventas y nuevamente se comunicó en la línea con Carlos Lozada Martínez, el supuesto gerente, quien explicó las condiciones de venta, que le mandaría un contrato y que debía depositar el pago, pero Jesús interrumpió la conversación con el reclamo de su dinero.

“Ayer pagué por una camioneta y no me ha llegado, quiero una explicación o quiero mi dinero”, reclamó. El supuesto gerente de ventas simplemente colgó el teléfono.

Jesús volvió a marcar, pero la llamada ya no entró, fue como si hubieran bloqueado sus números telefónicos, luego envió un correo electrónico como segunda opción para reclamar la devolución de su dinero y por ese mismo canal le contestaron con una amenaza de muerte.

“Te tenemos vigilado, sabemos todos tus datos, calladito te ves más bonito porque si hablas te mueres”, se lee en un mensaje que recibió en su e-mail.

En efecto, Jesús se sintió en riesgo porque para concretar la compra del vehículo que nunca recibió, tuvo que proporcionar sus datos y documentos personales que lo ubican e identifican.

El portal electrónico www.cementelca.com era una copia de la página auténtica de Cementos Cruz Azul y el domicilio fiscal de la empresa referido en el sitio, en ese entonces pertenecía a una bodega abandonada en la ciudad de Xalapa, Veracruz.

Las llamadas que hizo Jesús a los defraudadores tuvieron como destino la capital de Veracruz y las que él recibió de ellos también salieron de esa ciudad, de acuerdo con el detalle de llamadas desglosado en la factura de su teléfono celular.

Un expediente de denuncia que contiene documentos certificados por la CNBV evidencia cómo en la sucursal Banorte 4202 con domicilio en Michoacán, el ejecutivo, Abraham Ceja Pérez abrió una cuenta bancaria con una identificación falsa a nombre de Ana Castillo Gómez, la supuesta representante legal de Cementos Cruz Azul. Como comprobante de domicilio utilizó un recibo de Telmex con una dirección en Morelia, y remitió el estado de cuenta a una dirección distinta también en esa ciudad.

Los propietarios del comprobante de domicilio rechazaron haber aprobado el uso del documento para ese fin y aseguraron que Castillo Gómez no es miembro de su familia ni de sus amistades.

La institución bancaria no acató las leyes que le obligan a identificar a sus clientes, además por el monto y movimientos que registró la cuenta bancaria, debió avisar a la CNBV de posibles actos irregulares y sospechosos en la banca, tal como lo indica la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, conocida como Ley Antilavado. Sin embargo, ésta cerró la cuenta una vez que llegó a ceros.

De febrero a marzo de 2015, la cuenta bancaria a nombre de Ana Castillo Gómez recibió en total 320 mil pesos por parte de cinco personas que cayeron en el fraude y depositaron por la compra de vehículos a Cementos Cruz Azul y Barcel.

El dinero se movió en montos de 7 mil 856.39 pesos, a las ganancias de las casas de juegos Fiesta Casino Benavides y Golden Investment, así como a la empresa Corporación Turística N, todos en Lima, Perú, donde los pesos pasaron a soles y luego a dólares hasta agotar el saldo de la cuenta.

El sitio electrónico estuvo activo de enero a diciembre de 2015, periodo en el que cambió teléfonos de contacto y domicilios en Veracruz, Guadalajara, Xalapa, Puebla y la Ciudad de México.

Los ciberdelincuentes usan dominios gratuitos o de paga en los que habilitan portales electrónicos clonados de instituciones públicas y privadas bien posicionadas.

Recurren a los bancos para abrir cuentas con identidades falsas y sistemas internacionales y electrónicos de pago que usan para recibir y mover el dinero que obtienen de los defraudados.

Con su testimonio, las víctimas narran estafas con el mismo modo de operación y con movimientos bancarios similares en Banorte, Banamex y Scotiabank, que abrieron cuentas a nombre de Mariana Ferrer Espinosa, Ana Castillo Gómez, Víctor Rubén Sáenz Lomelí y Juan Jacobo Salazar, para recibir depósitos como pago por el falso remate de flotillas.

Jesús presentó una denuncia con pocas probabilidades de recuperar su dinero porque el ministerio público y policías de investigación, antes de intentar esclarecer el delito y buscar un culpable, juzgaron su exceso de confianza e ingenuidad; asegura que hasta se rieron de él.

“La última vez que fui a la procuraduría me dijeron que no pueden investigar porque todo fue por internet, que yo no vi a nadie cara a cara como para señalar físicamente a alguien, que había que corroborar la identidad de la titular de la cuenta en los sistemas del INE, que el banco no quería mandar la información de la cuenta bancaria y que el nuevo sistema penal da más derechos a los imputados que a las víctimas”, expresa.

Le advirtieron que obtener esa información no sería fácil por las leyes de protección de datos personales y el secreto bancario.

Cuando la procuraduría solicitó la colaboración del Instituto Nacional Electoral (INE) para corroborar la identidad de Ana Castillo Gómez, en virtud de que existía una investigación por un fraude y ella era sospechosa, el organismo respondió que no podía brindar esa información porque su padrón está sujeto a la protección de datos personales.

Así que, por la actitud de los investigadores, la reacción de las instituciones y porque recibió amenazas de muerte de los supuestos representantes de Cementos Cruz Azul, Jesús prefirió abandonar el trámite de su denuncia.

Confiesa también que la experiencia lo hizo pensar en suicidarse, se sentía en la quiebra económicamente y a la fecha no tolera que se burlen de él, que lo tachen de “pendejo” cada vez que narra su experiencia. Para él, es mejor dejarlo en el olvido y no volver a hablar del tema.

“No niego mi responsabilidad, pero fui víctima de un delito que existe por la corrupción, si el banco no hubiera abierto una cuenta para robar dinero, si alguien evitara las páginas falsas, si en mercadolibre no existiera lo ilegal; pero no, aquí el único culpable soy yo y antes que ser una víctima, para todos soy un pendejo”.

La ruta de México a Perú, lavado de dinero

La ruta que recorrió el dinero de Jesús, de México a Perú y el cómo ingresó a las ganancias legítimas de los casinos, es una modalidad de lavado de dinero, de acuerdo con lo que describe el Grupo de Acción Financiera Internacional (GAFI) en su informe: *Las Vulnerabilidades del Sector de Casinos y Juegos de Azar 2009*.

Además, se trata de delincuencia transnacional que la Organización de las Naciones Unidas (ONU) definió en 1995 como los "delitos cuya iniciación, prevención y efectos directos o indirectos afectan a más de un país"[7], y enlistó en ellos el lavado de dinero, actividades terroristas, robo de arte y cultura, tráfico de armas, secuestro de aviones, crimen informático, y otros.

"El ecosistema criminal es poderoso y complejo. Igual que las compañías de servicios en línea, está fragmentado en muchas organizaciones pequeñas y especializadas".[8]

Y así como las empresas destinan recursos y personal para implementar un área de ciberseguridad dedicada a proteger los datos que guardan de posibles ataques cibernéticos, por el lado de los ciberdelincuentes hay programadores, hackers, matemáticos, ingenieros y demás especialistas que saben cómo romper los esquemas criptográficos más avanzados.

Clonar una página electrónica implica dolo; y la forma de operar este sistema para cometer fraudes requiere de delincuencia organizada en el espacio físico y en el ciberespacio para consolidar el delito y luego para mover los fondos obtenidos ilícitamente.

El GAFI describe a los casinos como instituciones no financieras, pero que entre su operación con la oferta de entretenimiento realizan actividades que los hacen similares a una institución financiera; aceptan fondos en cuenta, intercambian dinero, realizan transferencias de dinero, cambio de moneda extranjera, servicios de valor almacenado, cambio de cheques; etc., servicios que tienen disponibles las 24 horas del día. Por estas características y servicios los casinos son vulnerables al blanqueo de capitales.

[7] Dondé, F. Delitos Transnacionales. Tirant lo blanch-Instituto Nacional de Ciencias Penales. México 2018. Pág., 20.
[8] Pisanty A. Llámame Internet. Caja Chica-Secretaría de Cultura. Junio 2018.

El organismo internacional explica que depositar fondos en una cuenta de casino es una *técnica* de lavado de dinero; el casino que administra la cuenta es el *mecanismo* para llevar a cabo el delito y los fondos depositados son el *instrumento*.[9] Aunque aclara que depositar fondos solo puede considerarse una acción ilegal cuando el dinero es producto de una actividad ilícita; y la *técnica*, el *mecanismo* e *instrumento* se unen para darle forma legal.

Asimismo, son indicadores de lavado de dinero utilizando cuentas de un casino: los depósitos frecuentes de efectivo, transferencias bancarias a la cuenta del casino, los fondos retirados de cuenta poco después de ser depositados, transacciones a la cuenta del casino realizadas por personas distintas del titular de la cuenta y el uso de terceros para realizar transferencias bancarias y estructuración de depósitos.

La forma en que se movió el dinero que Jesús depositó a la cuenta de Ana Castillo Gómez, supuesta representante legal de Cementos Cruz Azul, por la compra de una camioneta de flotilla que supuestamente remataba la cementera, reúne esas características.

Transfirieron los fondos a través de la banca electrónica hacia las cuentas de los casinos Fiesta Casino Benavides y Golden Investment, además de la firma Corporación Turística N., todos con domicilio en Lima, Perú.

Jesús depositó el dinero a las 10:59 horas del 11 de marzo de 2015; un total de 112 mil pesos. A las 04:12 horas del día siguiente hicieron cuatro transferencias con diferencias de segundos a la cuenta de Fiesta Casino Benavides, cada una por la cantidad de 7 mil 856.39 pesos.

Los días 13, 14, 15 y 16 del mismo mes y año, la cuenta a nombre de Castillo Gómez solo registró movimientos con cantidades mínimas por pagos a Paypal, disposiciones en cajero y cobro de comisiones por esas operaciones.

---

[9] En las metodologías e indicadores de lavado de dinero, el GAFI aplica los siguientes conceptos:
Método: un procedimiento particular para llevar a cabo actividades de lavado de dinero. Hay más distinciones en el concepto de método de lavado de dinero:
Técnica: una acción particular o forma en que se realiza la actividad, por ejemplo, comprando un cheque de caja.
Mecanismo: un sistema o cosa que lleva a cabo parte del proceso. Un ejemplo de mecanismo de lavado de dinero es un casino.
Instrumento: un objeto de valor (o valor representativo) que se utiliza de alguna manera en el proceso de lavado de dinero; por ejemplo, un cheque de casino o fichas de casino.

El día 17, la cuenta bancaria recibió dos depósitos más, cada uno por 70 mil pesos que se sumaron al dinero previamente depositado por Jesús. A las 11:39 horas de esa fecha y con diferencia de segundos, hicieron siete transferencias, una por 7 mil 682.11 pesos y el resto por 7 mil 726.45, a la cuenta de la casa de juegos Fiesta Casino Benavides; y dos más por 7 mil 751.46 pesos, a la cuenta del casino Golden Investment S.A.

En suma, la cuenta bancaria a nombre de Ana Castillo Gómez recibió de febrero a marzo de 2015, la cantidad de 320 mil pesos, por parte de seis personas que compraron vehículos supuestamente a Cementos Cruz Azul y Barcel, fondos que fueron trasladados a través de la banca electrónica a los establecimientos en Perú.

Por ejemplo, el 20 de febrero a las 09:27 horas, recibió en México un depósito de 140 mil pesos por la compra de una camioneta a Cementos Cruz Azul.

Según el estado de cuenta expedido por el banco Banorte y certificado por la Comisión Nacional Bancaria y de Valores (CNBV), la cuentahabiente transfirió el dinero durante los tres días posteriores, en montos de 22 mil 874. 60 pesos, 7 mil 600 y 7 mil 731 pesos a los casinos Fiesta Casino Benavides, Golden Investment y la firma Corporación Turística N. También hizo pagos a MercadoLibre por 279, 135 y 320 pesos.

El seis de marzo, recibió otro depósito de 52 mil 500 pesos; luego uno más, el día nueve, por 30 mil pesos, y así en fechas posteriores recibió depósitos por la compra y apartados de vehículos que se movieron en horarios similares con diferencia de segundos hacia las cuentas de las tres empresas.

En los registros del Ministerio de Comercio Exterior y Turismo (Mincetur), organismo con sede en Perú, consta que la empresa Thunderbird Fiesta Casino Benavides es propietaria de la sala de juegos Fiesta Casino. La firma obtuvo en 2017 dos renovaciones para la explotación de juegos de casino y máquinas tragamonedas; explota 33 mesas de juego y 402 máquinas según las resoluciones directorales.

Inició actividades de juegos de azar y apuestas en julio de 2007 y desde 2016 expide comprobantes electrónicos y está inscrita al Régimen de Agente de Retención, de acuerdo con la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT)**.**

En octubre de 2017, la empresa chilena Sun Dreams compró el casino a la firma Thunderbird, junto con otros tres establecimientos del mismo giro, por un monto de 26 millones de dólares.

En la base de datos de la SUNAT, la firma Corporación Turística N., registra actividades "de alojamiento para estancias cortas" desde 2009 y no tiene actividad de comercio exterior.

Asimismo, ante el Mincetur, la empresa Golden Investment S.A., es propietaria del Casino Golden Palace, que en 2016 renovó su autorización para explotar 30 mesas de juego y 786 máquinas tragamonedas. Esta firma inició actividades de juego y apuestas desde mayo de 1997 y también desde mayo, pero de 2015 es emisor electrónico.

La descripción de cómo se movió el dinero, de México hacia los casinos en Perú, que obtuvieron los ciberdelincuentes por las estafas con el falso remate de flotillas por Internet podría configurar el delito de lavado de dinero. Sin embargo, las procuradurías locales, aunque no han resuelto ningún caso, llevan años en la investigación específica del delito de fraude con esas características; no hay indicio de que consideren la posibilidad de que detrás de esa estafa hay blanqueo de capitales.

El GAFI en su informe de evaluación más reciente sobre *Medidas anti Lavado y contra la Financiación del Terrorismo en México*[10], publicado en 2018, considera que a pesar de que el país produce buena inteligencia financiera, no posee una política integral y proactiva que priorice la investigación financiera y el procesamiento del lavado de activos como un delito autónomo.

"Las partes componentes -la inteligencia financiera, la investigación, el procesamiento y las sanciones- no están funcionando congruentemente para mitigar los riesgos de lavado de activos".[11]

Esto se traduce en una tasa de condenas, por lavado de dinero, extremadamente baja, condición que revela "un alto grado de ineficacia" en el modo en que se inician las investigaciones, sin

[10] Este documento ofrece un informe de las medidas de lucha contra el lavado de activos y financiamiento del terrorismo vigentes en México a la fecha de la visita in situ (28 de febrero al 16 de marzo de 2017). El GAFI aclaró que, en el transcurso, la Procuraduría General de la República (PGR) hoy Fiscalía General de la República (FGR) emprendió acciones para subsanar deficiencias, mismas que aún deben madurar.

[11] FATF y GAFILAT. *Medidas antilavado y contra la financiación del terrorismo-México, Informe de evaluación mutua*. FATF, Paris. 2018. Pág., 34.

fundamento; en cómo se conducen, con deficiencias de metodología de investigación, procedimientos extremadamente largos, falta de coordinación interna entre los diferentes organismos especializados a nivel federal y estatal y falta de experiencia.

"Las deficiencias identificadas, por ejemplo, la PGR no busca ninguna asistencia de manera proactiva a través de mecanismos de cooperación internacional cuando el delito tiene algún componente transnacional, tienen un impacto negativo sobre la investigación de lavado de activos".[12]

Por tanto, el organismo internacional recomendó a la Procuraduría General de la República (PGR), hoy Fiscalía General de la República (FGR), priorizar la investigación del lavado de dinero tal como prioriza el narcotráfico y delincuencia organizada; y considerar la importancia de tener acceso a herramientas de cooperación internacional con el fin de recabar evidencia de otros países y asegurar activos ubicados en el exterior.

El GAFI también sugirió a la FGR realizar investigaciones paralelas con la información que genera la Unidad de Investigación Financiera sobre otros delitos que pudieran representar riesgo de lavado de dinero.

El gobierno mexicano manifestó ante el GAFI que cuando hay fundamento para creer que se cometió un delito determinante, la FGR inicia una investigación y persigue penalmente ambos delitos juntos; no obstante, el organismo internacional observó que las cifras "cuentan otra historia" y que se puede inferir que cuando la unidad de competencia inicia una investigación por corrupción o delincuencia organizada, muy rara vez inicia una investigación paralela sobre blanqueo de capitales.

Por ejemplo, en 2016 la FGR reportó dos mil 173 averiguaciones previas por tráfico de drogas, mil 702 por corrupción, 455 por delitos fiscales y apenas 178 por lavado de dinero.

Así, el GAFI concluyó que la FGR no persigue casos de lavado de activos internacional complejos y que las autoridades no son proactivas en la búsqueda de asistencia para la cooperación internacional de manera adecuada y oportuna para perseguir el lavado de activos y los delitos determinados asociados que tengan elementos transnacionales, como consecuencia

[12] *Idem*. Pág., 39.

de la falta de capacidad para realizar investigaciones financieras paralelas y priorizar el rastreo de activos.

Tras un clic cientos de víctimas

De 2014 a 2019 otras 526 personas, siete empresas y una escuela primaria, aparte de Jesús, David, Rosa, Escribano, Isaac, Norberto y Edgar cayeron y son víctimas, en México, del fraude cibernético transnacional operado con Internet con el falso remate de flotillas y portales electrónicos ficticios. Bastó un clic para que todos cayeran en la estafa.

Por este tipo de fraude los ciberdelincuentes obtuvieron en ese mismo periodo, por lo menos 57 millones 268 mil 940 pesos. El monto está calculado sobre información detallada que se obtuvo de 245 denuncias de un total de 523 que existen en las procuradurías y fiscalías estatales, interpuestas por quienes, por Internet, fueron engañados para comprar un vehículo de flotilla en remate y no lo recibieron.

Las cifras de por sí impresionantes representan apenas una mínima parte de la capacidad de operación alcanzada por los ciberdelincuentes en el territorio mexicano y de la rentabilidad que les deja el fraude cibernético en esa modalidad.

Asimismo, es una minúscula fracción de la dimensión del problema que desafía al país para la persecución de la ciberdelincuencia transnacional y de la impunidad que beneficia a los ciberdelincuentes.

Estos números corresponden al periodo del 01 de enero de 2014 al día 30 del mismo mes, pero de 2019, conseguidos a través de solicitudes de acceso a la información pública presentadas a las 32 procuradurías y fiscalías locales del país, así como a la Fiscalía General de la República (FGR).

Como casos individuales vislumbran fraudes aislados en los estados, pero observados en conjunto evidencian un crimen global bien planeado y operado con Internet que traspasa las fronteras mexicanas.

Vía transparencia, se solicitó que cada procuraduría informara sobre el número de denuncias por fraude cibernético, específicamente con el falso remate de flotillas ofertadas en portales electrónicos clonados y perfiles falsos empresariales en redes sociales; los montos del fraude en cada denuncia; el género de la víctima; el estado actual de la indagatoria a fin de conocer si hay

detenidos o sentenciados por esta actividad ilícita y el proceso legal hacia las páginas electrónicas para inhibir o prevenir más estafas de este tipo.

Los resultados reflejan solo una parte de la realidad porque no todas las dependencias respondieron a las solicitudes en los términos en que fueron planteadas. Mientras unas proporcionaron información perfectamente detallada porque privilegiaron el principio de máxima publicidad, algunas no contestaron, otras argumentaron que no poseen estadísticas que distingan este delito del fraude tradicional y que no están obligadas a generarlas para satisfacer al solicitante, o bien, indicaron que en las leyes locales no existe un delito relativo al "fraude cibernético" y si existe, es del orden federal y por tanto la investigación es responsabilidad de la FGR.

"No se cuenta con registro de denuncias por el delito de Fraude Cibernético, toda vez que se trata de un delito del orden federal", respondió; por ejemplo, la Fiscalía General de Morelos.

En contradicción, la FGR alegó que investiga y persigue "delitos federales" con características relacionadas con los delitos contemplados en el Código Penal Federal de México (CPF) y demás leyes especiales.

El artículo 386 del Código Penal Federal dice que "comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido".

El delito de fraude está tipificado, entonces debe considerarse fraude cibernético a la misma conducta delictiva pero que se comete y desarrolla con Internet y el uso de medios informáticos y dispositivos digitales.

Aunque la ley no diga textualmente fraude cibernético, en los casos analizados sí se configura un fraude y es una conducta punible.

Esto no significa que las autoridades no persigan el fraude operado y consolidado con herramientas cibernéticas, pero si refleja que enfrentan barreras y obstáculos que jurídicamente hablando vuelven obsoletos sus procedimientos porque no están acorde con la nueva realidad tecnológica; están desfasados y se tornan inoperantes. Ese es el problema.

El mecanismo judicial de ir al juez para que declare si hubo daño o no y que después resuelva en juicio la culpabilidad del imputado, está rezagado ante la velocidad de los medios digitales utilizados para delinquir.

Con Internet, el daño a la víctima de un delito ya no es totalmente localizado, la afectación se incrementa y potencia impresionantemente; y por un fraude que ocurre en México resulta complicado que el juez notifique al posible sospechoso que está; por ejemplo, en Perú.

La consecuencia de los procedimientos lentos ante la velocidad de Internet perjudica indirectamente a la víctima ya de por sí afectada directamente por el delito cibernético; tal como ocurrió con Rosa N.

Rosa es una mujer empresaria que radica en Guadalajara; la ilusión de adquirir un vehículo a menor precio que en el mercado tradicional, la llevó a creer en un remate de flotillas que hacía el Grupo Modelo a través de su página electrónica, pero también se trataba de una estafa.

En Internet se encontró con el anuncio de la supuesta empresa cervecera, llamó para pedir informes y acordó la compra de una camioneta que le llegaría al día siguiente a su domicilio. Se quedó esperando porque la unidad nunca llegó.

"La primera vez si me dijeron que podía ir a verla a la cervecería, pero ya después me dijeron: 'no, no se preocupe nosotros se la enviamos. Usted nada más confírmenos el depósito, inmediatamente nos llama o le llamamos y se la enviamos", relató.[13]

Al no recibir el vehículo, Rosa fue a la dirección exhibida en el sitio electrónico; se encontró con que sí pertenecía a una cervecera, pero no a la que ella le había comprado la camioneta.

"El vigilante de la cervecería me dijo luego, luego que me vio y que le pregunté ¿Aquí es donde rematan carros? '¡Hay no, otra más que cae!'".[14]

Transcurrido el tiempo rechaza hablar de aquella experiencia. En una breve comunicación vía telefónica, su hija, solo lamentó que haya caído en ese fraude cibernético.

[13] Rosa N., contó su experiencia en diciembre de 2015, cuando Televisa buscó su testimonio para una nota de alerta sobre esta modalidad de fraude. *Gangas de autos por internet, nueva estafa en México.* Noticieros Televisa.
[14] *Idem*

“Esa fue mi madre, pobrecita de ella que cayó en ese fraude y le robaron su dinero, pobrecita”, expresa.

La mujer empresaria fue víctima del fraude en noviembre de 2015, ese año relató su experiencia a Televisa; casi cuatro años después su caso no ha sido resuelto. Ante la televisora aseguró que cuando denunció no le dieron ninguna esperanza a pesar de que la Fiscalía de Jalisco ya conocía el modo de operación de este delito y sabía que los ciberdelincuentes transferían los fondos obtenidos hacia Perú, según lo explicó en su momento el fiscal general, aunque no precisó el lugar exacto.

“La mayoría de ellos son de origen colombiano y peruano. Crean o abren cuentas bancarias en el sistema bancario mexicano y llevan a la gente a hacer transferencias a estas cuentas que inmediatamente las transfieren en este caso a Perú. Estamos revisando los cómplices que puedan tener aquí en México”, declaró Eduardo Almaguer, en ese entonces fiscal general de Jalisco.[15]

Como víctima, Rosa no está incluida en las estadísticas obtenidas vía transparencia para esta investigación, porque la Fiscalía General de Jalisco respondió con una “declaratoria de inexistencia de información” a la solicitud de acceso a la información pública presentada.

La Unidad de Transparencia argumentó que no localizó información que cumpliera con las especificaciones requeridas y de la que según hizo una búsqueda exhaustiva en las bases de datos de la Dirección General de Inteligencia, Política Criminal y Prevención del Delito; la Dirección General de Delitos Patrimoniales y Financieros, y la Fiscalía Especial Regional.

En 2015, el entonces fiscal general de esa entidad, Eduardo Almaguer, declaró a Televisa que ese año la dependencia a su cargo había acumulado hasta diciembre 77 denuncias por ese tipo de fraude, y en 2014 registró 127.

Sin embargo, para 2019 la misma dependencia declara inexistente esa información pese a que si existe en sus archivos.

[15] Eduardo Almaguer, fiscal general de Jalisco durante 2015, concedió en ese año una declaración a Televisa para una nota informativa de alerta sobre el fraude con remates de flotillas por Internet. *Gangas de autos por internet, nueva estafa en México.* Noticieros Televisa.

La Fiscalía General del Estado de Puebla entregó una respuesta similar; informó que recibió 5 denuncias "por fraude en sitios web y redes sociales" durante 2018 y ninguna en años anteriores, empero en esta entidad también existen antecedentes por este delito, al menos desde 2015.

La diferencia de respuesta de las procuradurías y fiscalías ante la solicitud de acceso a la información pública hace que las cifras citadas en esta investigación representen una mínima parte de la capacidad alcanzada por los ciberdelincuentes que integran y mueven toda la estructura digital necesaria para cometer el fraude con el remate de falsas flotillas y trasladan el dinero de México a Perú.

En conjunto, las fiscalías que respondieron con mayor precisión a las solicitudes de acceso a la información pública, con privilegio al principio de máxima publicidad, reportaron 523 denuncias en agravio de 526 personas, 7 empresas y una escuela, por el delito de fraude con las características de un remate de flotillas a través de páginas electrónicas ficticias, redes sociales y mercados electrónicos.[16]

Por ejemplo, la Fiscalía General del Estado de Chihuahua (FGEC) posee en su departamento de Información Cibernética de la Dirección de Análisis de Evidencia Digital e Informática Forense, una base de datos que de 2014 a 2018 registra 124 denuncias por el delito de "fraude" por la venta de "flotilla de carros", "maquinaria" y una "motocicleta", operado con Internet y el uso de la red social de Facebook, anuncios clasificados en un periódico local, correos electrónicos falsos, además de plataformas de mercado electrónico como MercadoLibre, Vivastreet, VivaAnuncios, Autocosmos, SegundaMano y Trovit.

[16] Para esta investigación fueron descartadas las respuestas que proporcionaron fiscalías y procuradurías locales por las siguientes razones:
De los estados de Campeche y el Estado de México, porque proporcionaron estadísticas del delito de fraude en general sin distinguir del fraude cibernético.
Sonora rechazó la solicitud porque "no existe un tipo penal en el Código Penal para el Estado de Sonora relativo al fraude cibernético".
Chiapas, Durango, Guanajuato, Nuevo León, Oaxaca, Sinaloa y Veracruz, argumentaron que no existe en sus registros información sobre el fraude cibernético y no están obligados a generarla.
San Luís Potosí, Tlaxcala, Baja California Sur, Colima, Guerrero y Nayarit respondieron a la solicitud de acceso a la información pública, pero no fue posible descargar el archivo de la Plataforma Nacional de Transparencia. Se solicitó el archivo directamente en sus unidades, sin respuesta.
Hidalgo no contestó, la Fiscalía de Morelos argumentó que el fraude cibernético es facultad de la FGR y su similar de Jalisco declaró una inexistencia de información.

Para cometer el fraude los ciberdelincuentes también utilizaron páginas electrónicas entre las que aparecen: www.mineramfrisco.com, www.mineranaica.com, www.motomundoamerica.com y www.g-mexico.com.

"En lo que se refiere a medio por el que operan, se refiere (sic) a sitios de internet que son utilizados por los presuntos sujetos activos del delito de fraude, vía internet, lo cual no significa necesariamente que estos sean falsos o apócrifos; o en su caso se pueden dar de alta para operar a través de las plataformas de los mismos", precisa la FGEC.

Los cuatro portales electrónicos antes mencionados ya están desactivados en el ciberespacio y tienen antecedentes por fraude cibernético por el remate de falsas flotillas. En su momento fueron reportados como sitios electrónicos clonados de los auténticos.

A través de la solicitud de acceso a la información pública presentada a la FGEC, se conoce que las víctimas en Chihuahua fueron defraudadas por montos que van desde los mil pesos hasta un millón 41 mil 448 pesos por la compra de vehículos, una motocicleta, flotillas y maquinaria pesada. Tres de los defraudados pagaron en dólares.

La FGEC continúa la investigación de los 124 fraudes, para ello recolectó con "herramientas abiertas" datos sobre las páginas electrónicas, correos electrónicos y redes sociales "para solicitar a la empresa información donde esté el dominio alojado".

Las fiscalías de Tamaulipas, Yucatán y Tabasco identifican también en sus bases de datos el fraude cibernético con internet y el falso remate de flotillas. El primer estado reportó un caso; y el segundo14, entre enero de 2018 y enero de 2019.

Tabasco registró 7 denuncias, 2 de ellas en 2017; el mismo número en 2018; y tres en los primeros meses de 2019, operados con los portales electrónicos ficticios, maquinaria y sumunistrosagricolasmf.com, maquinaria-importadora.com, seminuevos-neuholland.com.mx, halliburton-mexico.com.mx y el mercado electrónico mercado.mx, donde utilizaron el nombre de Bimbo.

El registro del testimonio de las víctimas ante esas dos instituciones narra el modo de operación: "En internet ofrecen en venta vehículos de medio uso que provienen de una flotilla, paga por el auto y no se lo entregan", "Refiere el denunciante que un organismo gubernamental subastaría varios vehículos, él lo paga y no se lo entregan", "Por medio de Facebook se interesa por un

vehículo de subasta de Grupo Modelo, lo paga y no se lo entregan", "En Mercado libre contacta un vehículo de la flotilla de la empresa grupo Modelo, no se lo entregan".

Los fraudes ocurridos en Yucatán, los operaron con páginas en Facebook y los portales electrónicos: www.cemexventas.org, www.gamesa-mexico.com, www.bonattimexico.mx y otros con la imagen corporativa de Bayer, Grupo Modelo, La Costeña, Gamesa y Soriana.

Las fiscalías que tienen bien identificado este tipo de fraude cibernético no han esclarecido ninguno de los casos; además porque no es su facultad tampoco desactivaron ninguno de los portales electrónicos utilizados, solo los reportaron a la plataforma de Google destinada a la prevención del *Phishing* como se denomina al método que usan delincuentes cibernéticos para estafar y obtener información confidencial de los usuarios de internet a través de la suplantación de identidad.

Según las estadísticas de Google, la tendencia del *phishing* se incrementó desde 2007; al corte de noviembre de ese año, recibió tres mil 800 reportes por sitios de suplantación de identidad. Al cierre de febrero de 2019, acumuló 32 mil 454.[17]

De manera independiente y en correspondencia con sus políticas, Google determina o no la remoción del contenido.

Bajar del ciberespacio una página electrónica diseñada para suplantar a otra que es legítima y cometer delitos, requiere de la orden de un juez y para ello es necesario que las fiscalías presenten la evidencia del delito.

Bloquear los sitios electrónicos ficticios utilizados para el fraude con remate de flotillas, es una de las barreras que enfrentan las procuradurías para la persecución de ese delito y a ello se suma la definición de la jurisdicción.

A diferencia del espacio físico, en el ciberespacio la Internet extiende los territorios, prácticamente no existen las fronteras, característica que hace más difícil definir la jurisdicción; es decir, la zona geográfica donde ocurre el fraude cibernético.

[17] Google. *Informe de Transparencia*. https://transparencyreport.google.com/ . Consultado en mayo de 2019.

Antes era claro, si se cometía un fraude se ubica a quien lo comete y a la víctima, y a partir de ahí se define la jurisdicción, ahora para esta misma conducta ilícita cometida por medios virtuales, ese mecanismo es inoperante.

En el ciberespacio es difícil rastrear dónde ocurrió el fraude, quién es el autor intelectual o material, y luego considerar si las plataformas digitales o proveedores de servicios de almacenamiento en Internet son corresponsables del delito, dado que entre sus políticas de funcionamiento ofrecen mecanismos de confianza para los usuarios.

Cooperación internacional la red débil de México

Con el uso de una página *web* o algún portal de comercio electrónico se comete un fraude cibernético; la víctima hizo compras en México, pero el sitio electrónico tiene un *hosting* en Colombia; el estafador se encuentra en Perú, quien además usó líneas telefónicas que contrató en Estados Unidos para establecer comunicación con la víctima. La víctima denuncia el fraude en México donde la conducta delictiva está tipificada, pero el delito operado con Internet y dispositivos digitales, en sí se cometió en Colombia y la evidencia se queda dividida entre México, Colombia, Perú y Estados Unidos.

Este escenario corresponde a un delito cibernético transnacional porque traspasa las fronteras de una nación a otra y sus efectos directos o indirectos afectan a más de un país. ¿Qué autoridades se hacen cargo de investigar ese delito y en qué legislación deberán basarse para reunir y tratar la evidencia, así como juzgar el caso?

La respuesta está en la cooperación internacional entendida como el apoyo que se prestan dos o más instituciones, sean gobiernos, empresas u organizaciones de la sociedad civil para enfrentar fenómenos globales.

La cooperación internacional se consolida con la transferencia, recepción e intercambio entre países, de información y conocimientos, de recursos tecnológicos, económicos, humanos o legales, con el objetivo de incrementar su capacidad en el intento de enfrentar y superar dificultades que perjudican a más de un país.

El cibercrimen afecta a más de un país. Si bien los avances tecnológicos como el Internet trajeron múltiples ventajas para la humanidad, también provocaron efectos nocivos porque son aprovechados por las redes de delincuentes que en el ciberespacio operan de un país a otro en cuestión de minutos.

“Frente a esas manifestaciones de criminalidad, su transfronterismo y su notable flexibilidad, aparece la incapacidad de los estados nacionales para enfrentarlas. En todos esos casos, los delincuentes no solo rebasan el ámbito de un sistema nacional de justicia penal que debería

proteger a la víctima, sino además los estados-nación han perdido casi por completo la capacidad de proteger a sus ciudadanos".[18]

En 1999 en el marco de la Organización de los Estados Americanos (OEA), los Ministros de Justicia y Procuradores Generales de las Américas reunieron a un grupo de expertos sobre delito cibernético que realizó un diagnóstico de la actividad delictiva en el ciberespacio en los estados miembros, así como un análisis de la legislación, las políticas y las prácticas nacionales sobre cibercrimen.

El grupo de expertos también identificó a las entidades nacionales e internacionales con experiencia en prevención y combate de la ciberdelincuencia, y los mecanismos de cooperación para enfrentarla.

El diagnóstico concluyó que la mayor dificultad que enfrentan los países miembros de la OEA ante el delito cibernético es la carencia de entidades especializadas y con facultades para investigarlo y perseguirlo, y la falta de capacitación suficiente para formalizar actividades exhaustivas y coordinadas contra el cibercrimen.

Es decir, que para la investigación de los cientos de denuncias que existen en México por el fraude cibernético con el falso remate de flotillas ofertadas a través portales electrónicos ficticios, las procuradurías y fiscalías locales requieren de cooperación internacional para obtener la evidencia digital y seguir la ruta del dinero de México hacia Perú, porque no tendrían los recursos económicos para financiar un viaje a sus investigadores hacia ese país.

Las ventajas del Internet para la ciberdelincuencia representan retos para los gobiernos, las legislaciones e investigadores, porque deben incrementar sus recursos y capacidad en la persecución y sanción de los delitos cibernéticos.

Desde 1999 cuando surgió el Grupo de Trabajo en Delito Cibernético de las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA), a través de la OEA, promueve la capacitación sobre el contenido y alcance de las convenciones y disposiciones internacionales en materia de delito cibernético, el manejo de

[18] Dondé, F. *Delitos Transnacionales.* Tirant lo blanch-Instituto Nacional de Ciencias Penales. México 2018. Pág., 31.

fuentes abiertas para la investigación de los delitos informáticos, la evidencia digital, como asegurarla y garantizar la preservación de la cadena de custodia.

El adiestramiento del que México ha sido beneficiario incluye también el manejo de las pruebas digitales, legislación procesal relacionada con delitos cibernéticos y la importancia de la cooperación jurídica internacional para su persecución y sanción.

Debido a que el cibercrimen afecta a las sociedades de todo el mundo por su actual dependencia a las tecnologías de la información, la OEA recomienda a sus países miembro, entre ellos México, adherirse al Convenio sobre la Ciberdelincuencia del Consejo de Europa.

El también conocido como Convenio de Budapest, creado en 2001 y ratificado en 2004, es el único acuerdo internacional que prevé el derecho penal, procesal y la cooperación internacional como áreas esenciales para la investigación, persecución y sanción del delito cibernético; y considera de carácter prioritario la formalización de una política penal similar contra la ciberdelincuencia en cada uno de los países miembros. Actualmente 56 países se han adherido al convenio como si integraran una red de lucha contra el cibercrimen.

México está fuera de esa red porque no ha formalizado el proceso para sumarse al Convenio Budapest, a pesar de que es observador desde 2007, de que el país es vulnerable al cibercrimen y de que la incidencia de delitos en el ciberespacio crece cada año.

En 2016 durante el Foro para la Gobernanza de Internet, el responsable de la división de ciberdelincuencia del Consejo de Europa y secretario del Comité del Convenio de Budapest, Alexander Seger, exhortó a autoridades mexicanas a adherirse y dejar de ser observadoras.[19]

A decir de investigadores de delitos cibernéticos, la adhesión de México al Convenio de Budapest permitiría avanzar en el tema de cooperación internacional contra el cibercrimen, además de fortalecer la legislación nacional y otras regulaciones. Actualmente la transnacionalidad de los ciberdelitos y la falta de tratados internacionales que faciliten el cruce de fronteras representan obstáculos en la investigación y persecución de ciberdelincuentes.

[19] Hernández A. *Piden a México en Convenio de Budapest, ser más que un observador.* Periódico Excelsior. https://www.excelsior.com.mx/hacker/2016/12/07/1132670 . Consultado en mayo 2019.

En su artículo 23, el Convenio de Budapest establece los principios generales relativos a la cooperación internacional con la que compromete a las partes a cooperar entre sí en la mayor medida de lo posible en la aplicación de los instrumentos nacionales pertinentes para las investigaciones y procedimientos relativos a los delitos relacionados con sistemas y datos informáticos para obtener pruebas en formato electrónico de esos ilícitos.

“Necesitamos reaccionar rápido”

Si los investigadores de las fiscalías reaccionaron rápido, seguramente saben que el portal electrónico www.cementelca.com lo registraron el 20 de enero de 2015 con la dirección IP 23.236.62.147, que lo actualizaron el 22 de marzo y que el nueve de diciembre también de 2015 lo bajaron del ciberespacio. Todo ese tiempo, los ciberdelincuentes lo usaron para cometer fraudes cibernéticos con el falso remate de flotillas con la imagen corporativa de Cementos Cruz Azul, pero era un clon de la página electrónica auténtica de la cementera.

Si los investigadores no actuaron con agilidad una vez que recibieron las denuncias de las víctimas de la estafa, a esta fecha habrán perdido toda esa evidencia digital porque ya no está disponible en el ciberespacio, al menos no en herramientas abiertas para la investigación de ciberdelitos.

En los sitios que ofrecen el servicio de hosting y registro de dominios ya está libre esa dirección electrónica; es decir, que cualquiera la puede usar si paga por ella, pero en su historia llevará el antecedente de que fue utilizada por el cibercrimen.

En opinión de Andrés Velázquez, presidente y fundador de MaTTica, el primer laboratorio de investigación de delitos informáticos en América Latina con sede en México, se acostumbra la vieja usanza contra el cibercrimen y las autoridades no entienden que en el nuevo mundo de la sociedad de la información es necesario hacer eficientes y rápidos los procesos para darle certidumbre jurídica tanto a los afectados del fraude cibernético como a la marca que involucran los ciberdelincuentes.

Esa rapidez que requiere la investigación del cibercrimen, remarca, incluye la cooperación internacional porque se trata de delincuencia transnacional.

“En los medios digitales la evidencia digital es sumamente frágil y si no reaccionan rápido, pues no es así como que la escena del crimen vaya a quedar durante semanas.

“Y no es un tema de México, es un tema internacional. Hoy en día el cometer un delito con tecnología es mucho más rápido, entonces necesitamos reaccionar también rápido, y eso significa cooperación internacional porque estamos hablando de un delito transfronterizo donde parte de la evidencia está en otra parte del mundo, entonces cómo nos hacemos de esa

información y cómo logramos traer esa información a nuestro país de una forma validada desde su origen hasta acá", explica.[20]

Tan rápido como opera la delincuencia con Internet deben reaccionar las autoridades para la investigación de los ciberdelitos, sofisticar sus métodos y estrategias tal como lo hacen los ciberdelincuentes para no ser rastreables.

Sin embargo, no ocurre así; en México existen desde 2014 centenares de denuncias por el delito del fraude cibernético transnacional con el falso remate de flotillas en portales electrónicos ficticios que todavía investigan las procuradurías y fiscalías locales. Los casi cinco años transcurridos no reflejan rapidez para la obtención de la evidencia digital que es seguro ya desapareció del ciberespacio y tampoco para desactivar los portales electrónicos ficticios a fin de evitar más estafas.

En mayo de 2019, tras emitir una alerta por la detección del portal www.fordplanta.mx, utilizado para el fraude, la Policía Federal (PF) argumentó que el registro de estos sitios con proveedores en el extranjero complica su inhabilitación.

"El Centro Nacional de Respuesta a Incidentes Cibernéticos CERT MX de la Policía Federal ha inhabilitado en varias ocasiones diversos sitios apócrifos; sin embargo, luego de un tiempo los vuelven a subir a la red en otro servidor, en algunos casos a través de un proveedor fuera de México, lo que dificulta el proceso de inhabilitación".[21]

Con el sitio www.fordplanta.mx, ciberdelincuentes suplantaron el portal electrónico www.ford.mx propiedad de la armadora Ford, con la intención de hacer fraudes cibernéticos ya no con el remate de flotillas, sino de automóviles seminuevos y autos demo, nueva variante de su actividad ilícita.

"La Secretaría de Seguridad y Protección Ciudadana informa que, a través del monitoreo de la Red Pública de Internet, elementos de la División Científica de la Policía Federal detectaron el portal www.fordplanta.mx, el cual suplanta la identidad de una empresa automotriz y puede ser

[20] Entrevista con Andrés Velázquez, presidente y fundador de MaTTica, el primer laboratorio de investigación de delitos informáticos en América Latina, elaborada el 26 de marzo de 2019.
[21] Comunicado de prensa emitido por la Secretaría de Seguridad y Protección Ciudadana. *Policía Federal alerta sobre fraude cibernético a través de sitio falso de empresa automotriz.* Mayo 09 de 2019.

usado en un esquema de fraude mediante la adquisición de bienes inexistentes, en este caso la venta de vehículos".[22]

"Gran remate de autos demo 2017 y 2018", dice el anuncio de la portada de la página *web* www.fordplanta.mx en la que colocaron el correo electrónico ventas@fordplanta.mx y el número de teléfono 6624920150, como canales de comunicación.

El número de teléfono corresponde a una línea fija con domicilio en Hermosillo, Sonora, contratada con el proveedor UC Telecomunicaciones, S.A.P.I. de C.V., según información obtenida con herramientas abiertas del Instituto Federal de Telecomunicaciones (IFT).

Aunque la Secretaría de Seguridad y Protección Ciudadana (SSyPC) y la PF alertaron sobre la actividad fraudulenta de la página electrónica, no la desactivaron. El dominio www.fordplanta.mx fue registrado el 24 de abril de 2019 con el proveedor de dominios y hosting GoDaddy.com; y días después de la alerta seguía activo.

En 2018, víctimas del fraude cibernético de esta modalidad, también reportaron la operación de ciberdelincuentes con el portal electrónico www.fonatur.org, una copia del sitio electrónico oficial del Fondo Nacional de Fomento al Turismo (Fonatur) alojado con el dominio www.fonatur.mx.

En septiembre de ese año, el Fonatur denunció penalmente ante la Fiscalía General de la República (FGR) el mal uso de su nombre, logotipo e imágenes.

"El Fondo Nacional de Fomento al Turismo (FONATUR), informa a la opinión pública, que detectó el uso indebido del nombre, logotipos e imágenes de FONATUR, en un portal no oficial del que desconoce su titularidad, con la liga www.fonatur.org, en el que se ofrecen unidades vehiculares y de maquinaria pesada por medio de subastas electrónicas; acciones ajenas a los objetivos, funciones y facultades de FONATUR".[23]

El proceso legal no fue significativo contra los ciberdelincuentes que administraban el portal ficticio; éste permaneció activo hasta el mes de diciembre. Lo registraron el cuatro de julio de

[22] *Idem*

[23] Comunicado de prensa 14/2018 del Fondo Nacional de Fomento al Turismo. *Fonatur presenta denuncia por el uso indebido de su nombre, logotipo e imagen.* 13 de septiembre de 2018.

2018 y realizaron una actualización el dos de septiembre para cambiar el domicilio y el teléfono con el que se comunicaban con las víctimas del fraude.

Velázquez dice que "no es un secreto" que existen ciberdelincuentes dedicados a crear páginas electrónicas con dominios similares a empresas grandes y con mucha reputación; y se valen del derecho a la privacidad y protección de datos personales del que gozan cuando los registran ante la Corporación de Internet para la Asignación de Nombres y Números (ICANN por sus siglas en inglés)[24], para ocultarse de los que hacen investigación cibernética.

En caso de que no paguen por un hosting y dominio, vulneran uno ajeno para insertar una página ficticia sin que el propietario del dominio principal se percate.

Y así como manipulan los dominios electrónicos en Internet, hacen lo mismo con las líneas telefónicas debido a que actualmente existen las que funcionan con sistemas y herramientas de privacidad que benefician a los delincuentes.

"Tienen líneas telefónicas con número, pero las utilizan por internet y para contratarlas no necesitan identificación. La línea la compran; por ejemplo, en Canadá con un número 01800 en México, puedes conectarte a una red de wifi y usarla, hasta se puede programar como si fuera una empresa y que te conteste 'gracias por llamar a tal si quiere hablar a administración marque uno', pero marcas tres veces y siempre te contesta la misma persona", expone.

Una vez lista la página electrónica ficticia y demás infraestructura tecnológica para el fraude, los ciberdelincuentes mueven el contenido entre los cibernautas para hacerlo viral y captar víctimas. En esta etapa del delito usan Facebook y otras redes sociales.

"Se meten a la mejor a pagar anuncios en Facebook y tratar de pasar la liga de la página entre amigos, de pásala, pásala, pásala para que se haga viral. No es caro anunciarse en Facebook y es muy redituable. Todo es muy barato, por un año puedes comprar dominios hasta en seis dólares; tener una página (electrónica) te puede costar diez dólares, o sea, no es una inversión

[24] ICANN es una corporación pública sin fines de lucro con participantes de todo el mundo dedicados a mantener Internet seguro, estable e interoperable. Promueve la competencia y desarrolla políticas sobre los identificadores únicos de Internet. A través de su función de coordinación del sistema de nombres de Internet, tiene un impacto importante en la expansión y evolución de Internet. www.icann.org

tan grande comparado con lo que obtienen por el enganche o apartado del auto. La rentabilidad es muy alta", agrega.

El investigador de delitos cibernéticos insiste que enfrentar a los ciberdelincuentes depende de la reacción rápida de las autoridades.

Refiere que en 2017 y 2018 el Laboratorio de Investigación de Delitos Informáticos bajo su dirección, atendió hasta dos casos por mes de empresas afectadas por el mal uso de su marca e identidad digital para el fraude cibernético. "Le ocurrió a Bimbo, a Sabritas, a muchísimos".

Las firmas implementaron estrategias de ciberseguridad que les alertan cuando en el ciberespacio alguien registra un dominio similar a su nombre corporativo; esto les permite pararlo a tiempo.

Las compañías prefirieron protegerse por su cuenta que recurrir a las autoridades para tratar de bajar la página por el mal uso de su marca, porque ese proceso habría tardado hasta dos años.

"Nos hace falta entender más claro que en estos temas tiene que ser mucho más dinámica la persecución de este tipo de delitos; dos, que requerimos de cooperación internacional porque si no, no se puede hacer; y tres, que hay que castigar la conducta no el medio".

Según él, aquellos que piensen que hay que castigar el internet porque es un medio para cometer delito, están mal; el delito también lo pudieron haber hecho si alguien llegaba a la puerta y decía 'oye, vengo de cementos cruz azul, estoy vendiendo coches de esta flotilla, este te cuesta tanto', hubiera sido exactamente lo mismo.

Recalca que Internet en el ciberespacio no es una vida alterna al espacio físico porque en ambos espacios se manifiestan las mismas conductas, lo único que cambia es el medio.

¿Hay esperanza para las víctimas de este fraude?, se le pregunta.

-Yo creo que si hay esperanza si logramos que sea eficiente la forma de obtención de pruebas y cooperación internacional en un mundo digitalizado, y estamos hablando de mayores capacidades y nuevos procesos. Estamos acostumbrados a la vieja usanza. Voy a tratar de contestarlo de una forma diferente, sin meterme en ninguna bronca. Me buscan y me dicen que por qué en México el tema de delitos informáticos es tan lento y por qué en Estados Unidos es rápido, y mi primera respuesta es que no es que sea rápido, es diferente. En Estados Unidos si

llega alguien y dice oye es que ella me robó dinero por internet y no hay una legislación de ello, el juez dice: '¿Está afectando a esta persona?, sí; ¿Es algo malo?, sí; ¿Si lo repite es malo?, pues sí. Ah pues va a haber un castigo'. En el caso de los latinos es: '¿Tenemos una ley?, no'; vamos a tener que reformar la ley y ahí se queda. Necesitamos entender el proceso, que hay cosas que están escritas y otras que no, y ahí tenemos el área de oportunidad.

¿En la legislación está el área de oportunidad?

-En la legislación, en los procedimientos y en la cooperación internacional.

Añade que detrás del fraude cibernético sí hay alguien; que a pesar de las barreras que la misma tecnología permite, el internet no es tan anónimo y si se hacen las investigaciones correctas se puede ubicar al responsable y una forma de lograrlo "es seguir el dinero".

"Las víctimas a pesar de que hayan caído en esa situación, deberían tener la certeza jurídica de que se persiga quién del otro lado lo está haciendo, pero se escudan en el no entiendo para decir es que no se puede, es que es Internet, pero entonces por qué el gobierno está poniendo accesos públicos de internet para que las personas se conecten. Para mí los accesos en los parques y demás, es miren aquí cuántos delincuentes podemos tener".

Internet para todos ¿Y la ciberseguridad?

Que los mexicanos tengan acceso a internet para disminuir la brecha entre los conectados y no conectados, es desde 2013 un mandato constitucional sustentado en el artículo sexto de la Constitución mexicana.[25] A partir de ese año, el gobierno promovió la implementación de Internet para todos.

Surgió la Estrategia Digital Nacional para digitalizar[26] al país con zonas de conexión a Internet gratuito y la distribución de dispositivos de acceso; que todos los habitantes de México estuvieran conectados.

El Internet es ahora una herramienta indispensable de vida, omnipresente, la usamos por todos lados. Está en nuestras casas, en las calles con los sistemas de videovigilancia; en el salón de clases, lo llevamos en nuestros bolsillos con el teléfono celular y otros dispositivos móviles.

Hay Internet en nuestras computadoras, entró a los televisores, empieza a acompañarnos a bordo del automóvil y con la llegada del Internet de las cosas el refrigerador y la estufa no tardan en estar conectados. ¿Y la ciberseguridad?

La primera Estrategia Nacional de Ciberseguridad en México (ENC) se publicó en 2017, cuando ciberdelincuentes ya operaban con Internet y en el ciberespacio habían montado una estructura cibernética para hacer fraude con portales electrónicos ficticios y el falso remate de flotillas de vehículos corporativos, se tiene antecedente de ellos desde 2014; es decir, le llevan ventaja al Estado.

Pero el fraude cibernético no es el único ciberdelito, el cibercrimen usa Internet para robo de identidad, ciberespionaje, fraudes a la banca, evasión de impuestos, distribución en línea de pornografía infantil y materiales que incitan el odio racial, captan víctimas para la trata de

[25] Artículo 6, apartado B, fracción I de la Constitución Política de los Estados Unidos Mexicanos: El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales.

[26] La digitalización se define como la capacidad de un país y su población para usar tecnologías digitales que permitan generar, procesar y compartir información; asimismo, se relaciona con el concepto que describe las transformaciones sociales, económicas y políticas asociadas con la adopción masiva de las TIC. Estrategia Digital Nacional 2013-2018.

personas laboral o sexual, y hoy en día las campañas de desinformación y las *Fake News* representan una conducta antisocial en el ciberespacio.

El tema de ciberseguridad[27] en México apareció tarde en la agenda pública si se considera que desde 2013, académicos y expertos reunidos en el Primer Encuentro Latinoamericano sobre Ciberseguridad: Delitos Cibernéticos e Informática Forense, con sede en la Facultad de Derecho de la UNAM, advertían que las actividades del crimen cibernético debían verse como asuntos de seguridad nacional.

Para ese año, el gobierno mexicano ya conocía también las dimensiones del cibercrimen en el país porque la Policía Federal, a través de la División Científica atendió 51 mil denuncias ciudadanas y más de 200 mil incidentes cibernéticos; desactivó cerca de 17 mil sitios fraudulentos y emitió más de 2 mil alertas de ciberseguridad dirigidas a instituciones públicas y privadas.[28]

En 2014, la Organización de Estados Americanos (OEA) estimó con el estudio Tendencias de Seguridad Cibernética en América Latina y el Caribe, que los costos inherentes a la comisión de los delitos informáticos alrededor del mundo ascendieron a 113 mil millones de dólares y en México representaron 3 mil millones de dólares.

Aún con ese panorama, se publicó la primera estrategia de ciberseguridad en 2017 con la visión de hacer de México, hasta 2030, una nación resiliente ante los riesgos y amenazas en el ciberespacio.

Con el cambio de gobierno, del expresidente Enrique Peña Nieto al presidente Andrés Manuel López Obrador, el tema de ciberseguridad y el uso de Internet, de ser una estrategia plasmada en un documento de 31 hojas se redujo a un párrafo de cinco líneas que dice que "mediante la instalación de Internet inalámbrico en todo el país se ofrecerá a toda la población conexión en carreteras, plazas públicas, centros de salud, hospitales, escuelas y espacios comunitarios".[29]

---

[27] *Ciberseguridad:* Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación. *Estrategia Nacional de Ciberseguridad. México 2017.*

[28] *Estrategia Nacional de Ciberseguridad.* México 2017. Pág., 14.

[29] *Plan Nacional de Desarrollo 2019-2024.* Pág., 52

Significa que la prioridad es extender la cobertura de Internet en el país y conectar al ciberespacio a los más que se pueda, sin que exista en México una estrategia de ciberseguridad consolidada con la visión de proteger primeramente a los usuarios, del cibercrimen.

En el territorio mexicano hay 71.3 millones de habitantes conectados a Internet[30] con diferentes dispositivos; el más recurrente es el smartphone. El 96.9 por ciento de los cibernautas usan Internet para obtener información.

Navegan en un ciberespacio que carece de ciberseguridad; entiéndase este concepto como la protección del espacio cibernético a través de estrategias, normas, mecanismos de control, procedimientos legales y métodos de gestión de riesgos disponibles para proteger el intercambio de información que hacen por Internet, los individuos, las organizaciones y las instituciones públicas y privadas.

Dentro de la ciberseguridad debe incluirse la ciberdefensa que implica la protección del ciberespacio desde una perspectiva de seguridad nacional. La ciberseguridad y la ciberdefensa representan en el ciberespacio al ciberpoder que es la facultad del Estado mexicano de proteger la soberanía nacional en el entorno digital.

El ciberespacio es en sí, la cuarta dimensión de operaciones de seguridad de la inteligencia civil, policial, militar y naval constituida como ciberseguridad pública.

En opinión de Arturo García Hernández, especialista en ciberseguridad del Banco de México, el país no avanza en esta materia porque cada seis años se reinventa una estrategia para proteger el espacio digital.

"Pasan los años, cambiamos de sexenio y lo que vemos es que, desafortunadamente, México sigue a la mitad de la tabla. México ahora ronda en un nivel dos o tres de madurez en ciberseguridad. ¿Qué quiere decir esto? Que, a lo largo del tiempo, no importa el indicador y no importa lo que estamos haciendo, si no lo sostenemos, lo que logramos es tener un país a media tabla".[31]

[30] De acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2018.

[31] Riquelme, R. *"En ciberseguridad, estamos reconstruyendo a México cada seis años".* El Economista, 24 de febrero de 2019.

Asegura que México se posiciona a la mitad de los principales indicadores que miden el nivel de protección del ciberespacio.

Por ejemplo, en 2015 la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) publicó su Índice Mundial de Ciberseguridad (IMC)[32] en el que evaluó las medidas jurídicas, técnicas y de organización; capacidades humanas y la cooperación internacional de 193 países. México ocupó, en ese año, el lugar 18 de 29 clasificaciones; en 2017 alcanzó la posición 28 de 162 y quedó incluido en la categoría "Madurando", pero lejos de Singapur o Estados Unidos, líderes en ciberseguridad.

En su libro *CiberMéxico: Voluntades y Acciones en el Ciberespacio,* García Hernández describe que el nivel de madurez de la estrategia y política nacional en materia de ciberseguridad evoluciona de forma desordenada y mal definida.

Los rubros de cultura y sociedad; educación, capacitación y habilidades; marcos jurídicos y reglamentos; y normas, organización y tecnología que son parte de la estrategia de ciberseguridad, también tienen un nivel de madurez que evoluciona de forma desordenada, mal definida, y además con poca toma de decisiones de inversión de recursos.

Considera que el país posee los recursos humanos, tecnología y conectividad suficientes para empatar a los países que figuran en los primeros lugares de los índices de ciberseguridad, el problema es que se reconstruye cada que hay cambio de gobierno federal.

"La política pública que hace falta es mantener una estrategia de ciberseguridad a largo plazo. Estamos construyendo algo, ahí vamos y de repente, otra vez, volvemos a destruirlo y empezamos otra vez. Cambian las cabezas, los procesos, los protocolos y volvemos a comenzar. Creo que eso es algo que le ha hecho mucho daño a México", dice.[33]

[32] "El IMC tiene sus raíces en la Agenda sobre Ciberseguridad Global de la ITU y considera el nivel de compromiso en cinco ámbitos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional. El resultado es un índice a nivel de país y una clasificación mundial de la preparación para la ciberseguridad. El IMC no pretende determinar la eficacia ni el éxito de una medida particular, sino simplemente la existencia de estructuras nacionales para implementar y promover la ciberseguridad*". Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar (IMC).* ITU Ginebra 2015.

[33] Riquelme, R. *"En ciberseguridad, estamos reconstruyendo a México cada seis años".* El Economista, 24 de febrero de 2019.

México carece de una estrategia de ciberseguridad bien afianzada pese a que el gobierno tiene intención de proteger el ciberespacio; esto pone al país en rezago frente a naciones que formalizaron sus estrategias en años anteriores y que en 2019 las actualizan en concordancia con la evolución digital.

España; por ejemplo, formalizó en 2013 su Estrategia Nacional de Ciberseguridad (ENC) y en abril de 2019 anunció la actualización del documento para ampliar el concepto de ciberseguridad hacia una perspectiva de protección y defensa de los usuarios de internet. Antes la ENC de ese país protegía exclusivamente a las máquinas de conexión y dejaba a los cibernautas su propia seguridad y defensa en el ciberespacio.

Ingeniería social el cibercrimen perfecto

Manipular a las personas antes que, a cualquier sistema informático, es el crimen cibernético más efectivo. Se llama ingeniería social.

En el contexto de la seguridad informática, es la técnica para generar el entorno psicológico para engañar a la víctima y que, al maniobrar con sus emociones, una vez que se tiene contacto con ella a través de Internet, haga lo que el ciberdelincuente quiere que haga; por ejemplo, que deposite dinero, que envíe sus datos y documentos personales, que mande fotografías íntimas o videos con contenido sexual. La ingeniería social funciona con la premisa de que es más fácil engañar a alguien para conseguir información y dinero, que pasar horas tratando de violar un sistema de seguridad cibernética.

Esta técnica está incluida en la serie de ataques cibernéticos porque arremete directamente contra el usuario de Internet considerado el eslabón más débil del ciberespacio. Los ciberdelincuentes juegan con las emociones de sus víctimas.

El fraude cibernético del falso remate de flotillas ofertadas en portales electrónicos ficticios es un ejemplo. Con engaños, los estafadores consiguieron datos personales y dinero, y no hicieron más que contestar las llamadas que por su cuenta hicieron los cibernautas afectados tan pronto vieron los anuncios de los automóviles a precio de ganga. Generaron en ellos confianza y luego les crearon la urgencia de pagar por una camioneta porque si no lo hacían otro se las ganaría.

“Las camionetas y los autos se han vendido muy rápido, del modelo que usted quiere solo nos queda una y ya casi se vende, pero si de verdad la quiere comprar apóyenos depositando el cincuenta por ciento y se la apartamos hasta por diez días, la pasamos a bodega, o si paga todo completo se la mandamos a su domicilio sin ningún costo extra. Se han vendido muy rápido”, esta fue la estrategia que usaron los ciberdelincuentes cuando Norberto llamó a la supuesta planta de Petróleos Mexicanos (Pemex) que remataba sus vehículos de flotilla.

“Tiene un precio de 56 mil 500 pesos, lo tenemos por lote completo o por unidad. Tenemos alta reputación, se está comunicando a una empresa bastante grande. Cuando haga el pago se va a dirigir a la torre 25 con su váucher de transferencia bancaria y ya pasaríamos al patio vehicular, sino se presenta con el váucher no tendría acceso a la torre”.

La ingeniería social no surgió con la invención de las computadoras ni los sistemas digitales; los timadores, estafadores, defraudadores y otros delincuentes tienen éxito gracias a la manipulación dolosa de sus víctimas. Y así como antes iban a las plazas comerciales, a los parques o deambulaban por la calle en busca de una presa, ahora migran del espacio físico al ciberespacio, al fin las personas padecen las mismas debilidades con y sin internet, pero esta herramienta digital disminuye la probabilidad de ser identificado.

"La mentira ha adquirido nuevo nombre y dimensión en Internet, donde el riesgo para quien engaña es menor que cara a cara. Las estrategias se han complicado, "ingenierizado". Profesionales del tocomocho (estafa), espías industriales, 'crackers', escritores de virus, bromistas y, en general, la estructura abierta y confiada de la red han convertido a la ingeniería social en el crimen más difícil de combatir".[34]

La ingeniería social inicia con el sabotaje; en el ciberespacio el ciberdelincuente crea un sistema ficticio o una estructura de engaño que sirve para acercarse al usuario de Internet hasta ganarse su confianza.

A la fase del sabotaje, le sigue una etapa de alerta; se genera en el usuario la sensación de miedo o de urgencia ante la que tiene que reaccionar y buscar una solución.

En la tercer y última fase, la de asistencia; el ciberdelincuente le ofrece al cibernauta esa solución.

Los ciberdelincuentes involucrados en el fraude cibernético del falso remate de flotillas a través de portales electrónicos clonados están preparados, conocen la jerga de una empresa y de su estructura corporativa, cómo responde el personal asignado a cada una de las oficinas y departamentos; y también prevén la reacción de su víctima. Aunque suene crudo para las víctimas de la estafa, esta es una estrategia de ingeniería social exitosa.

Los estafadores lograron su objetivo que sin duda era obtener documentos personales y dinero de las víctimas, y no tuvieron la necesidad de violar algún sistema de seguridad, no hicieron

[34] Molist M. *Ingeniería social: mentiras en la red.* http://ww2.grn.es/merce/2002/is.html consultado en mayo 2019.

más que manipular, con engaños, las emociones de quienes cayeron en la estafa e inducirlos a que por sí mismos depositaran el capital ya fuera en ventanilla o por transferencia bancaria.

Asimismo, que por correo electrónico enviaran copia de su credencial de elector y comprobante de domicilio. El dinero lo transfirieron a las cuentas de las casas de juegos en Lima, Perú; mientras que los documentos con datos personales probablemente les eran útiles para continuar la dinámica de abrir cuentas en el sistema bancario mexicano con el robo de identidad.

Kevin Mitnick, un famoso hacker estadounidense, dedicado a la consultoría y asesoramiento en materia de seguridad, afirma que las instituciones públicas y privadas podrán invertir todos los recursos posibles en herramientas de ciberseguridad para mantener a salvo la información que poseen de los ciberdelincuentes, pero no servirá de mucho sino se apuesta por la capacitación del factor humano, al que denomina el eslabón más débil de la cadena de seguridad en el ciberespacio.

"A pesar de los esfuerzos de los profesionales de la seguridad, la información en todas partes sigue siendo vulnerable y seguirá siendo vista como un objetivo de los atacantes con habilidades de ingeniería social, hasta que el eslabón más débil en la cadena de seguridad sea fortalecido, el eslabón humano".[35]

Mitnick considera que el uso de Internet para el comercio electrónico modificó "dramáticamente" la seguridad; sin embargo, el desplegar más tecnología no va a resolver el problema de la seguridad humana.

En el mundo de los expertos en ciberseguridad e ingeniería social, dicen que la computadora más segura es aquella que permanece apagada y aun así, siempre existirá la posibilidad de convencer a alguien para que la encienda, porque no hay un solo ordenador que no dependa de un ser humano.

"Muchos ataques de ingeniería social son complejos, implican una serie de pasos y una planificación elaborada, combinando una mezcla de manipulación y conocimientos tecnológicos.

[35] Mitnick, K. *The Art of Deception. Controlling de Human Element of Security.*

Pero siempre me parece sorprendente que un ingeniero social hábil pueda lograr su objetivo con un ataque simple y directo. Solo pedir directamente la información puede ser todo lo que se necesita".[36]

Entonces, en el ciberespacio, la dificultad total no son las máquinas, parte del problema es el factor humano; la gente, que requiere desarrollar educación y habilidades digitales enfocadas en cómo usar con seguridad las tecnologías de información y comunicación.

Cuando la Secretaría de Seguridad y Protección Ciudadana (SSyPC) alertó sobre el portal www.fordplanta.mx, el cual suplantó la identidad de la empresa automotriz Ford para un esquema de fraude mediante la venta de vehículos inexistentes, acompañó la alerta con una serie de recomendaciones: verificar el sitio oficial de la empresa; de ser posible, solicitar al vendedor la ubicación física donde se puede comprobar la existencia del vehículo; no entregar ningún documento que contenga información personal hasta validar la legalidad de la oferta.

Son hábitos de educación digital que debe adoptar el usuario de Internet antes que integrarse a la estadística de los delitos cibernéticos como consecuencia de las dificultades del Estado para perseguir y sancionar el cibercrimen.

No se trata de revictimizar a quienes han sido víctimas de ciberdelitos, sino de fomentar la corresponsabilidad del uso seguro del Internet en el ciberespacio, de empoderar al usuario con el reconocimiento de sus derechos digitales y técnicas de autoprotección porque de nada servirá tener la mejor estrategia de ciberseguridad proporcionada por las autoridades si las personas siguen publicando datos sensibles y no resguardan celosamente la información personal que puede perjudicar su vida si tiene mal uso.

Para la ciberdelincuencia todos los cibernautas son un objetivo. Decir a mí no me va a pasar no es una afirmación del todo acertada; en ocasiones una persona, a través de su personalidad digital, puede ser utilizada para llegar a otra más vulnerable.

Tras vivir la traumática experiencia del fraude cibernético del falso remate de flotillas a través de portales electrónicos ficticios, las víctimas navegan con mayor cautela en el ciberespacio cuando usan Internet. Aprendieron a validar un portal electrónico falso de uno auténtico; saben

[36] *Idem*

que cuando en la barra de direcciones hay un candado abierto el sitio electrónico es inseguro, evitan abrir correos electrónicos desconocidos, no exponen sus datos personales.

Y para evitar que otros caigan en la estafa, cada que se encuentran una página electrónica falsa la reportan ante las autoridades o a través de los botones de denuncia que habilitaron las redes sociales.

A su vez, las empresas adoptaron mecanismos de ciberseguridad que detectan a tiempo el registro de dominios con nombres similares a su identidad corporativa, además emiten alertas a los cibernautas para prevenir que sean víctimas del fraude cuando han detectado que sus portales electrónicos fueron clonados.

Los particulares y las grandes corporaciones adquieren mecanismos de autoprotección para colaborar en la construcción de un ciberespacio seguro y confiable.

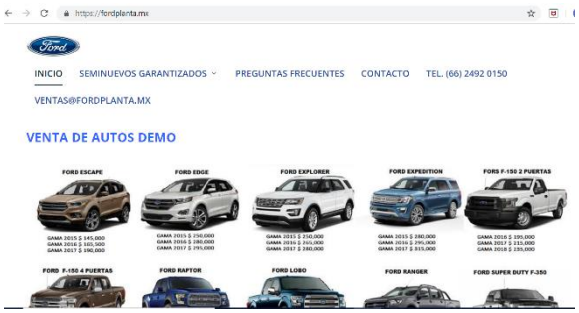
Eso no exime al gobierno de la obligación de desplegar una estrategia de ciberseguridad efectiva simultáneamente con su política de incrementar el acceso a Internet en el entendido de que las actividades en el ciberespacio, hoy en día, son necesarias para el desarrollo económico, social y educativo.

La ciberseguridad pública es la cuarta dimensión de operaciones de las corporaciones policiales con la que el Estado hará frente a la ciberdelincuencia y protegerá en el espacio cibernético las actividades de los cibernautas individualmente o constituidos como empresa, a fin de no solo dejar a ellos la responsabilidad de autoprotegerse.

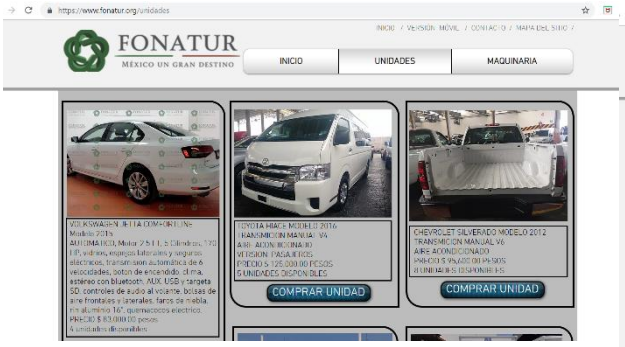
No custodiar el ciberespacio, no combatir el cibercrimen y tampoco sancionarlo, pondrá en evidencia el traslado de la inseguridad e impunidad del espacio físico al ciberespacio.

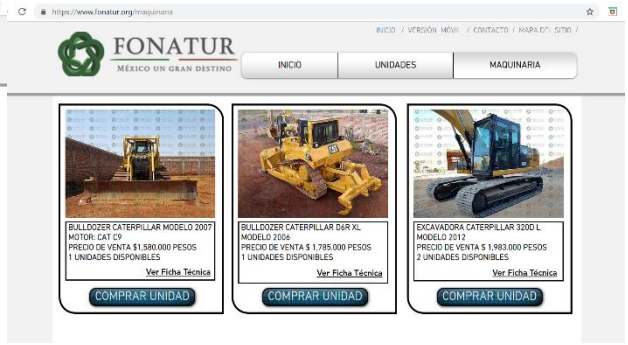
Anexos: falsos portales

Portal electrónico ficticio con el nombre de Ford (fordplanta.mx) utilizado para el fraude cibernético, en 2019, comparado con el portal auténtico de la armadora www.ford.mx

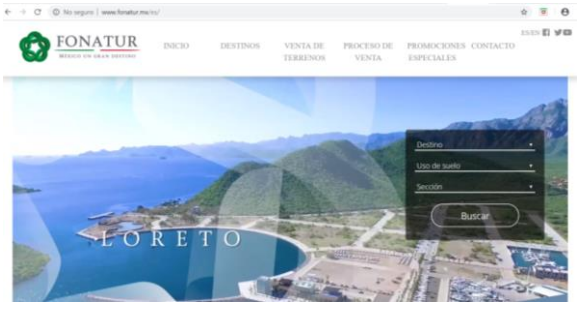


Portal electrónico ficticio con el nombre de Fonatur (www.fonatur.org), utilizado para el fraude cibernético en 2018.

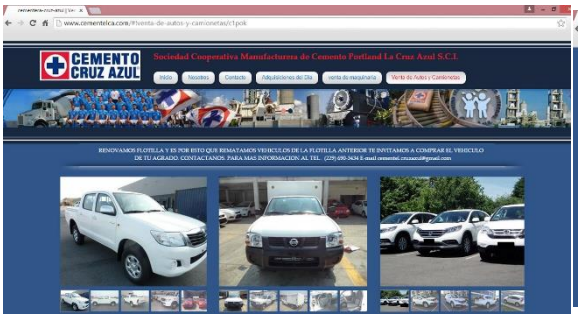


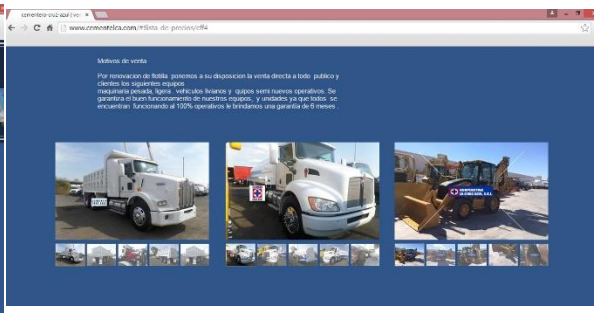


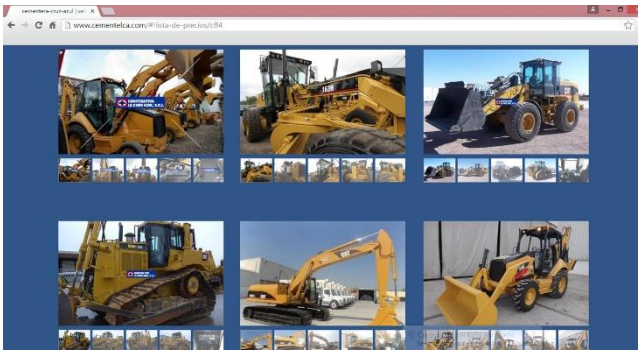
Portal electrónico auténtico de Fonatur www.fonatur.mx.



Portal electrónico ficticio con el nombre de Cementos Cruz Azul (www.cementelca.com) utilizado para el fraude cibernético en 2015; en ese año la cementera, desde su página *web* auténtica (www.cruzazul.com.mx), alertó sobre el mal uso de su identidad digital.







Bibliografía

* Dondé, F. *Delitos Transnacionales.* Tirant lo blanch-Instituto Nacional de Ciencias Penales. México 2018. Pág., 20.

* Mitnick, K. *The Art of Deception. Controlling de Human Element of Security*

*Pisanty A. *Llámame Internet. Caja Chica-Secretaría de Cultura. Junio 2018.* Pág., 20.

* Código Penal Federal de México.

* Constitución Política de los Estados Unidos Mexicanos.

* *Convenio sobre la Ciberdelincuencia del Consejo de Europa* (Convenio de Budapest).

* *Estrategia Nacional de Ciberseguridad*. México 2017. Pág., 14.

* Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2018. INEGI

* FATF y GAFILAT. *Vulnerabilities of Casinos and Gaming Sector*. March 2009.

* FATF y GAFILAT. *Medidas antilavado y contra la financiación del terrorismo-México, Informe de evaluación mutua.* FATF, Paris. 2018. Pag., 34.

* Google. *Informe de Transparencia*. https://transparencyreport.google.com/ .

* Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita

* Molist M. *Ingeniería social: mentiras en la red.* http://ww2.grn.es/merce/2002/is.html

*OEA. *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Informe Ciberseguridad 2016.

* *Plan Nacional de Desarrollo 2019-2024*. Pág., 52

* Riquelme, R. *"En ciberseguridad, estamos reconstruyendo a México cada seis años". El Economista*, 24 de febrero de 2019.

* Unión Internacional de Telecomunicaciones (ITU). *Índice Mundial de Ciberseguridad y Perfiles de Ciberbienestar (IMC)*. ABI Research. Ginebra 2015.