DICTAMEN EN SENTIDO POSITIVO QUE EMITE LA COMISIÓN DE SEGURIDAD CIUDADANA CON RELACIÓN A LA PROPOSICIÓN CON PUNTO DE ACUERDO POR LA CUAL SE EXHORTA A LA POLICÍA CIBERNÉTICA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, INVESTIGUE A LAS 130 APPS QUE DEFRAUDAN Y EMPLEAN COBRANZA ILEGITIMA A TRAVÉS DE DIFUNDIR LA DEUDA, Y EN ALGUNOS CASOS FOTOS O VÍDEOS, ENTRE SUS CONTACTOS, VIOLENTANDO LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS, PRESENTADA POR EL DIPUTADO JOSÉ GONZALO ESPINA MIRANDA, INTEGRANTE DEL GRUPO PARLAMENTARIO DEL PARTIDO ACCIÓN NACIONAL.

H. CONGRESO DE LA CIUDAD DE MÉXICO
II LEGISLATURA
PRESENTE:

NNS
HB

A la Comisión de Seguridad Ciudadana del Congreso de la Ciudad, II Legislatura, le fue turnada para su análisis y elaboración del dictamen respectivo a la **PROPOSICIÓN CON PUNTO DE ACUERDO POR LA CUAL SE EXHORTA A LA POLICÍA CIBERNÉTICA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, INVESTIGUE A LAS 130 APPS QUE DEFRAUDAN Y EMPLEAN COBRANZA ILEGITIMA A TRAVÉS DE DIFUNDIR LA DEUDA, Y EN ALGUNOS CASOS FOTOS O VÍDEOS, ENTRE SUS CONTACTOS, VIOLENTANDO LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS.** Presentada por el Diputado José Gonzalo Espina Miranda integrante del Grupo Parlamentario del Partido Acción Nacional.

En ese contexto y a fin de cumplir con lo dispuesto por lo establecido en el artículo 122, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; el articulo 30 numeral 1, inciso b de la Constitución Política de la Ciudad de México; el artículo 4 fracción XIV Bis, 5 Bis y 72 de la Ley Orgánica del Congreso de la Ciudad de México; el artículo 2 fracción XIV Bis, los artículos 56, 57, 57 Bis, 57 Ter, 103, 104 párrafos primero y segundo, 105, 106, 192 y 260 todos del Reglamento del Congreso de la Ciudad de México, la Comisión de Seguridad Ciudadana, encargada del análisis y dictamen de la Iniciativa con Proyecto de Decreto, desarrolló el trabajo correspondiente conforme a la siguiente estructura:

METODOLOGÍA

I.- En el capítulo "**ANTECEDENTES**" se da constancia del trámite y del inicio del proceso legislativo; así como de la fecha de recepción de los turnos para la elaboración del dictamen de la referida Iniciativa con proyecto de decreto.

II. En el apartado denominado **"PREÁMBULO"**, se exponen de manera sucinta, la motivación, fundamentación y alcances, de la propuesta en estudio y se hace una breve referencia a los temas que la componen.

III.-En el capítulo "**CONSIDERANDOS**", la Comisión expresa los argumentos de valoración de la propuesta y los motivos que sustentan la decisión.

IV.- Finalmente, en el capítulo "**PUNTOS RESOLUTIVOS**", la Comisión emite su decisión respecto de la iniciativa analizada.

NNS
HB

I. ANTECEDENTES

1. En sesión del Pleno del Congreso de la Ciudad de México, II Legislatura, en fecha 17 de febrero de 2022, el Diputado José Gonzalo Espina Miranda, presentó la **proposición con punto de acuerdo por la cual se exhorta a la policía cibernética de la secretaría de seguridad ciudadana de la ciudad de México, investigar las 130 apps que defraudan y emplean cobranza ilegitima a través de difundir la deuda, y en algunos casos fotos o videos, entre sus contactos, violentando la protección de los datos personales de los ciudadanos**, misma que a partir de esa fecha, fue publicada en la Gaceta Parlamentaria de este H. Congreso.

2. En esa misma fecha, la Mesa Directiva del Congreso de la Ciudad de México, II Legislatura, turnó a través del oficio **MDSPOPA/CSP/0723/2022**, para su análisis y dictamen, la **proposición con punto de acuerdo por la cual se exhorta a la policía cibernética de la secretaría de seguridad ciudadana de la ciudad de México, investigar las 130 apps que defraudan y emplean cobranza ilegitima a través de difundir la deuda, y en algunos casos fotos o videos, entre sus contactos, violentando la protección de los datos personales de los ciudadanos,** presentada por el Diputado José Gonzalo Espina Miranda, integrante del Grupo Parlamentario del Partido Acción Nacional.

3. Con fecha 22 de febrero de 2022, la presidencia de la comisión a través de los correos institucionales de las y los Diputados integrantes, remitió para su conocimiento la **proposición con punto de acuerdo por la cual se exhorta a la policía cibernética de la secretaría de seguridad ciudadana de la ciudad de México, investigar las 130 apps que defraudan y emplean cobranza ilegitima a través de difundir la deuda, y en algunos casos fotos o videos, entre sus contactos, violentando la protección de los datos personales de los ciudadanos**, que presentó el Diputado José Gonzalo Espina Miranda, integrante del Grupo Parlamentario del Partido Acción Nacional.

4. En sesión del Pleno del Congreso de la Ciudad de México, I Legislatura, en fecha 19 de mayo de 2020, se aprobó el Dictamen con proyecto de decreto por el que se adiciona la fracción XLV Bis al artículo 4 y el artículo 5 Bis a la Ley Orgánica del Congreso de la Ciudad de México, y se adiciona la fracción XLV Bis al Artículo 2; y se reforman y adicionan los artículos 56, 57, 57 Bis, 57 Ter y 329, así como las denominaciones del Título Cuarto y su respectivo Capítulo Primero y Sección Sexta, todos del Reglamento del Congreso de la Ciudad de México, en relación a las sesiones vía remota.

NNS
HB

5. El 06 de septiembre de 2021, la Junta de Coordinación Política del Congreso de la Ciudad de México, II Legislatura, mediante el ACUERDO CCMX/II/JUCOPO/04/2021, aprobó las REGLAS PARA DESARROLLAR LAS SESIONES VÍA REMOTA PARA EL PLENO, MESA DIRECTIVA, JUNTA, CONFERENCIA, COMISIONES, COMITÉS Y LA COMISIÓN PERMANENTE DEL CONGRESO DE LA CIUDAD DE MÉXICO, por lo cual se faculta a las Comisiones de este Congreso, las realizaciones de las sesiones ordinarias, extraordinarias o urgentes.

6. Con la finalidad de dar cumplimiento a lo establecido en la Ley Orgánica del Congreso de la Ciudad de México y su Reglamento, las y los diputados integrantes de la Comisión de Seguridad Ciudadana se reunieron de manera virtual, el 1 de abril de 2022 para discutir y votar el dictamen de la proposición del punto de acuerdo, con el propósito de someterlo a la consideración del Pleno de este Honorable Congreso.

II. PREÁMBULO

Esta Comisión es competente para conocer el presente Punto de Acuerdo de conformidad con lo dispuesto por los artículos 1, 3, 12, 13 fracción LXIV, 67, 70 fracción I, 72 fracción I, 74 fracción XLI, y 80 de la Ley Orgánica del Congreso; 84, 85, 86, 95 fracción II, 103, 104, 106, 187, 192, 221 fracción I, 256, 257, 258 y 260 del Reglamento del Congreso, ambos ordenamientos de la Ciudad de México.

III. CONSIDERANDOS

PRIMERO. Que la Constitución Política de los Estados Unidos Mexicanos, en su artículo 122, apartado A, establece que el ejercicio del Poder Legislativo se deposita en la Legislatura de la Ciudad de México, misma que se integrará en términos de lo que establezca la Constitución Política local.

SEGUNDO. Que la Constitución Política de la Ciudad de México, en su artículo 29, apartado D, de la Constitución de esta Ciudad establece las competencias del Congreso de la Ciudad de México:

"a) *Expedir y reformar las leyes aplicables a la Ciudad de México en las materias conferidas al ámbito local, por la Constitución Política de los Estados Unidos Mexicanos en las que se ejerzan facultades concurrentes, coincidentes o de coordinación con los poderes federales y las que no estén reservadas a la Federación, así como las que deriven del cumplimiento de los tratados internacionales en materia de derechos humanos y todas aquellas que sean necesarias, a objeto de hacer efectivas las facultades concedidas a las autoridades de la Ciudad".*

NNS
HB

TERCERO. Que el Artículo 13, fracción I de la Ley Orgánica del Congreso de la Ciudad de México, establece que el Congreso tiene competencias y atribuciones que le señalan la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política de la Ciudad de México, las Leyes Generales y la Legislación Local, aquellas que deriven del cumplimiento de los Tratados Internacionales en materia de Derechos Humanos en el ámbito legislativo.

CUARTO. Que la Propuesta de Punto de Acuerdo sujeta a análisis, en su exposición de motivos plantea lo siguiente:

*"**EXPOSICIÓN DE MOTIVOS***

ANTECEDENTES

***PRIMERO.-** El fraude a través de aplicaciones financieras donde ofrecen préstamos rápidos a las personas se ha disparado en México en los últimos seis meses hasta en un tres mil y para cobrar a sus víctimas esas "financieras" recorren al doxing es la práctica ilegal de revelar, por medios digitales, información personal sin el consentimiento de la víctima.*

El Consejo ciudadano de Seguridad y edificadas al menos 130 apps que defraudan y emplean cobranza ilegitima a través de difundir la deuda, y en algunos casos fotos o videos, entre sus contactos.

Los datos indican una tendencia al alza en esta modalidad del delito. En junio de 2021 se registró 10 reportes, y en enero de 2022 se reportaron 303 casos.

NNS
HB

***SEGUNDO. –** Salvador Guerrero Chiprés, presidente del Consejo Ciudadano expreso que "El esquema comienza con un ofrecimiento, en redes sociales, de préstamos fáciles y rápidos que se pueden tramitar por medio de aplicaciones de telefonía celular, en las que se solicita acceso al dispositivo del usuario. Al no cubrir el monto, los intereses de la deuda se elevan y se vuelven impagables.*

***TERCERO. –** Los reportes del organismo indican que el 64% de las víctimas son mujeres, el 56.5% de las personas tienen entre 26 y 40 años; 55% de los casos provienen de la Ciudad de México y el resto de otras entidades de la República como el Estado de México, Veracruz, Puebla, Jalisco o Tabasco.*

El Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México documentó 2 mil 231 reportes por fraudes y doxing en préstamos por medio de aplicaciones financieras, entre junio del año pasado y lo que va de este 2022 en todo el país.

El análisis de los reportes identifica a 130 supuestas financieras que se promueven en redes sociales y utilizan apps para el otorgamiento del crédito. Detalló que la asesoría jurídica gratuita permitió que, entre junio y enero, el Consejo Ciudadano apoyara a 173 víctimas en la apertura de una carpeta de investigación, el 92% de ellas por cobranza ilegítima, 3% por amenazas y el mismo porcentaje por extorsión.

C O N S I D E R A N D O S

Primero. *Que el párrafo tercero del artículo 1º de la Constitución Política de los Estados Unidos Mexicanos establece que:*

Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.

Segundo. *Que el artículo 14, Apartado B de la Constitución Política de la Ciudad de México, establece que:*

Toda persona tiene derecho a la convivencia pacífica y solidaria, a la seguridad ciudadana a vivir libre de amenazas generadas por el ejercicio de las violencias y los delitos. Las autoridades elaboraran políticas públicas de prevención y no de violencia, así como de una cultura de paz, para brindar protección y seguridad a las personas frente a riesgos y amenazas.

NNS
HB

Con base en lo anterior expuesto y fundado, se propone ante el pleno de este Honorable Congreso de la Ciudad de México, el siguiente:

PUNTO DE ACUERDO

ÚNICO. SE EXHORTA A LA POLICÍA CIBERNÉTICA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, INVESTIGUE A LAS 130 APPS QUE DEFRAUDAN Y EMPLEAN COBRANZA ILEGITIMA A TRAVÉS DE DIFUNDIR LA DEUDA, Y EN ALGUNOS CASOS FOTOS O VÍDEOS, ENTRE SUS CONTACTOS, VIOLENTANDO LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS"

SEXTO. Que el derecho a la protección de los datos personales de las y los ciudadanos tendrá que estar protegida por la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, así como lo manifiesta en su artículo 14, fracción II, el cual debe impulsar entre la sociedad la cultura y respeto por la seguridad y protección de los datos personales, y en la fracción IV, cita que se tienen que acordar mecanismos que disminuyan los riesgos del robo de datos, así como generar políticas que combatan este delito:

"Artículo 14. El Sistema Nacional, además de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable, tendrá las siguientes funciones en materia de protección de datos personales:

I.
II. Fomentar entre la sociedad una cultura de protección de los datos personales;

III.

IV. Acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendentes a cumplir con los objetivos y fines del Sistema Nacional, de la presente Ley y demás disposiciones que resulten aplicables en la materia;

NNS
HB

V. a la XXI."[1]

SÉPTIMO. Que el al artículo 1 de la LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR manifiesta que protegerá los intereses de todas las personas cuando reciban publicidad fraudulenta, donde se cometan abusos contra su persona como hostigamiento, amenazas u otro tipo de prácticas que atente contra la tranquilidad de las personas, pues las aplicaciones no solo fraudulentas, sino también la de empresas establecidas y oficiales cuando no reciben el pago de la persona que tiene la deuda comienzan a intimidarlas y a difundir la deuda con sus contactos de la persona:

"ARTÍCULO 1.- La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas, convenios o estipulaciones en contrario.

[1] Cámara de Diputados del H. Congreso de la Unión, (2017). *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS*. México

…
…

I. a la VI.
VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios.

VIII. a la XI.
…"[2]

OCTAVO. Que en el CÓDIGO PENAL PARA EL DISTRITO FEDERAL, considera como delito la cobranza y su mala práctica, cuando los medios para realizarla sean abusivos y se den por medio de intimidaciones, lo que incluye el acoso constante a la persona, cuando difunden la deuda por medio de sus contactos, incluso agregando la foto de la persona deudora por todos los medios posibles, también incurren en este delito cuando se divulgan sus datos personales, pues el hostigamiento se da por todos los medios posibles y de todas las formas posibles; el artículo 209 BIS menciona lo siguiente:

NNS
HB

"DELITO DE COBRANZA ILEGÍTIMA

ARTÍCULO 209 BIS. Al que con la intención de requerir el pago de una deuda, ya sea propia del deudor o de quien funja como referencia o aval, utilice medios ilícitos o efectúe actos de hostigamiento e intimidación, se le impondrá prisión de seis meses a dos años y una multa de ciento cincuenta a trescientos días de salario mínimo, además de las sanciones que correspondan si para tal efecto se emplearon documentación, sellos falsos o se usurparon funciones públicas o de profesión.

Para la reparación del daño cometido se estará a lo dispuesto en el artículo 46 de este Código."[3]

---

[2] Cámara de Diputados del H. Congreso de la Unión, (2019). *EY FEDERAL DE PROTECCIÓN AL CONSUMIDOR*. México

[3] Gaceta Oficial de la Ciudad de México, (2021). *CÓDIGO PENAL PARA EL DISTRITO FEDERAL*. México

NOVENO. Que la Secretaria de Seguridad Ciudadana tiene la obligación de monitorear la red para evitar cualquier tipo de delito cibernético que atente contra las y los ciudadanos, tanto su integridad física como psicológica, pues como se ha mencionado, las cobranzas ilegitimas o cobranzas falsas con apps se dedican a intimidar a las personas, a difundir sus datos personales e incluso con fotografías de la persona o videos; la policía cibernética de la Secretaria de Seguridad Ciudadana tiene que intervenir para localizar a las personas que mediante herramientas digitales y de forma fraudulenta se aprovechen de las personas realizando fraudes, pues esto no solo afecta de manera directa a su patrimonio, también de manera psicológica. Las autoridades se tienen que enfocar en este tipo de delitos que con el confinamiento han ido creciendo, pues la tecnología ya es necesaria para realizar pagos o movimientos bancarios, lo que ha llevado a que este delito se vuelva cada vez más normal.

Ahora bien, la Secretaría de Seguridad Ciudadana, como bien lo menciona cuenta con una unidad para prevenir delitos cibernéticos, así que es su obligación detener estas prácticas que cada vez afectan a miles de personas:

NNS
HB

"Una unidad cibernética formada el 3 de abril de 2013 con la finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes de la Ciudad de México.

Con los años el desafío ha ido en aumento, ya que las Tecnologías de la Información y de la Comunicación crecen y evolucionan de manera acelerada. Este ascenso influyó para que cada día más personas utilicen herramientas de internet con las que se puede acceder a un sin fin de información.

Por ello, la Policía Cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México busca, con estrategias de prevención, inculcar entre los cibernautas una cultura de respeto y "Civismo Digital"[4]

[4] https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica

DÉCIMO. Para entender el contexto de la gravedad de la difusión de datos personales de las y los ciudadanos por apps fraudulentas se menciona a continuación todo sobre el doxing y sus consecuencias graves, pues va mucho más allá del hostigamiento y de la difusión de datos personales, incluso los datos se difunden por diferentes países, lo que vulnera la vida completa no solo de la persona que identifico la app fraudulenta, también se encuentra en riesgo su familia; en lo que se refiere a las mujeres una vez difundida su foto o algún otro tipo de información comienzan a ser acosadas por personas extrañas, exponiéndose a ser atacadas fuera de su trabajo o casa, así que esto no solo queda un una app fraudulenta donde las autoridades tiene que retirarla y darla de baja, va mucho más alla de eso:

"Qué es el doxing? Definición

Una definición aproximada de doxing, que también podemos encontrar como doxxing, es que se trata de una práctica de ciberacoso que consiste en revelar información personal y confidencial de alguien a través de Internet.

Normalmente, el doxeo es el resultado de una venganza y quien lo lleva a cabo reúne toda la información y datos personales de su víctima, para hacerlos públicos en la Red, muchas veces incitando a otras personas a acosarla y, en el peor de los casos, convirtiéndose en amenazas reales contra la seguridad e integridad física de la víctima.

El significado de doxing está relacionado con la palabra «documentos», puesto que proviene de la abreviatura «docs» en referencia al document inglés. En 1990 los hackers acuñaron el término «dox» derivado de «docs» para referirse a la práctica de recopilar documentos o información personal de sus víctimas. Como veis, este tipo de práctica que mezcla ciberataque y ciberacoso viene ya de lejos.

El doxing puede llegar a ser muy peligroso, porque la información que se publica de las víctimas, facilita su identificación en el mundo real (muchas veces también la de sus familiares), su dirección postal, el lugar donde trabaja, su número de teléfono, etc. En el «mejor» de los casos, el resultado de un ataque de doxing es acabar suscrito algún servicio o recibir pedidos que la víctima no ha realizado. En el peor de los casos, se pueden recibir amenazas y más ciberacoso o ser víctimas de

suplantación de identidad o swatting (denuncias falsas a la policía en contra de la víctima, habituales en EE. UU.), entre otros tipos de ataques.

Objetivos del doxing

Pese a lo que pueda parecer, el objetivo del doxing no es chantajear a las víctimas para obtener dinero a cambio de no publicar la información personal recopilada. En este caso, lo que se pretende es hacer daño y, por tanto, publicar dicha información en Internet.

Esto se debe a que, como ya dijimos, detrás del doxing está la venganza, pero también la justicia extrajudicial o el dañar a personas con notoriedad y con las que se tienen opiniones o puntos de vista totalmente opuestos. Así, aunque cualquier persona puede ser víctima de doxing, son habituales los políticos, periodistas o personas con cierta notoriedad y presencia en redes sociales.

Aparte de hacer todo el daño posible a la víctima, el doxing también sirve para presionarla, para incitar a otras personas a que acosen a la víctima e incluso la amenacen, con el fin de intimidarla hasta el punto de que abandone la esfera pública.

NNS
HB

Cabe señalar, que según estudios realizados sobre la práctica de doxing, sus víctimas son mayoritariamente mujeres. De acuerdo a un informe de Amnistía Internacional, una de cada cinco mujeres en España afirma haber sido víctima de acoso en las redes y de estas, el 26% como mínimo una vez había sufrido doxing.

Consecuencias del doxeo

La principal consecuencia del doxing es la pérdida del anonimato en Internet, puesto que una vez que alguien empieza a doxear, información y datos personales de la víctima aparecerán en los principales foros de Internet (como Reddit o 4chan) y en muchas redes sociales, exponiendo la identidad de la víctima y la de sus familiares, así como dónde vive e incluso, en los casos más extremos, su rutina, su lugar de trabajo, sus costumbres, etc. Toda la información que haya podido encontrar el atacante, quedará expuesta en la Red.

Esta exposición puede llevar a consecuencias mucho peores, como ya hemos ido señalando, puesto que en muchos casos se incita al acoso de la víctima, a las amenazas, en definitiva, en poner en el punto de mira a una persona en concreto, con el fin de perjudicarla y creando en ella una sensación de inseguridad que le puede llevar a abandonar su presencia en la Red y cambiar incluso de vivienda.

¿Cómo protegernos del Doxing?

Puesto que el doxing consiste en la recopilación de información sobre la víctima, recopilación que se lleva a cabo a través de Internet, la mejor forma de protegerse es protegiendo lo más posible nuestra privacidad cuando navegamos y evitando dejar una huella digital demasiado rastreable.

NNS
HB

Lo mejor sería conectarnos a la Red usando una VPN para ocultar nuestra dirección IP, que es una de las formas de rastrearnos por Internet, pero no todo el mundo usa este tipo de redes privadas, por lo que la siguiente mejor opción pasa por ser precavidos.

Así, lo primero es procurar no usar el mismo nombre de usuario y contraseña para todas nuestras cuentas (sea en redes sociales, correos, plataformas de streaming, videojuegos en línea, foros, etc.), creando uno diferente para cada sitio al que estemos suscritos. Y cambiar de vez en cuando dichas contraseñas.

En ese sentido, también es recomendable no recurrir al crear cuenta usando nuestra cuenta de Facebook o Google, tan habitual y cómodo actualmente, porque estaremos «agrupando» información sobre nosotros en un «solo sitio». Si nos hackean una de estas cuentas, el hacker podrá tener acceso a todas aquellas que estén vinculadas a la misma.

Si usamos redes sociales, mantener nuestro perfil privado y procurar no compartir demasiada información personal en ellas, como, por ejemplo, donde trabajamos o fotografías de nuestros hijos.

Si somos usuarios de foros en Internet, nunca debemos usar nuestro nombre real en ellos y optar siempre por un seudónimo.

Procurar no revelar información personal o privada en redes sociales, foros o en grupos de mensajería instantánea.

En definitiva, se trata de evitar que por la Red circulen datos e información personal que pueda llevar a identificarnos.

¿Cómo se lleva a cabo el doxing?

A la hora de explicar cómo hacer doxing, debemos tener en cuenta que existen dos fases, la de recopilación de información y la de publicación.

NNS
HB

En la primera fase, los hackers (o doxxers) recopilan toda la información que puedan encontrar de las víctimas, rastreando redes sociales, páginas webs, bases de datos que puedan contener teléfonos y direcciones, pirateo de bases de datos, ataques de ingeniería social. El objetivo es reunir toda la información posible sobre la víctima, su entorno y su vida.

En la segunda fase se lleva a cabo la difusión de toda la información recopilada, utilizando todos los medios y plataformas disponibles en la Red. El objetivo es que la publicación llegue al mayor número de personas y que estas a su vez, sigan difundiéndola.

Tipos de doxing

Estos son los tipos de doxing más comunes que se producen en Internet:

- *La publicación de información personal y privada de una persona en la Red e identificación de la misma.*
- *Publicar en línea información confidencial y desconocida previamente de una persona.*
- *Publicación de información en línea con el fin de dañar la reputación de la víctima, así como la de sus asociados o allegados.*
- *Incitar el acoso y la intimidación de la víctima.*

- *Llevar a cabo una supuesta justicia personal, al exponer la identidad de supuestos criminales.*
- *«Doxing periodístico» cuando periodistas o medios recurren a esta práctica para investigar ciertas personalidades anónimas.*

Ejemplos de doxing

Ahora que ya sabes qué es y cómo funciona el doxing, vamos a ver algunos ejemplos reales de doxing.

Empezamos casi por el principio de esta práctica. En 1997, activistas antiaborto de EE. UU. se hicieron con información personal de las clínicas y profesionales que llevaban a cabo esta práctica en el país, publicándola en una lista negra que estuvo colgada en Internet hasta 2002. En ella no solo se identificaba a estas personas, también si incitaba a hacerles daño.

NNS
HB

Seguimos en EE. UU., pero en el año 2013; tras el atentado de la Maratón de Boston, miles de usuarios en Reddit decidieron jugar a ser policías y tratar de identificar a los responsables. Al final, lo que consiguieron fue identificar erróneamente a varios sospechosos, a los que sometieron a ataques de doxing. Ninguna de estas personas era responsable del atentado. Lo peor, es que a causa del acoso recibido, una de ellas acabó suicidándose.

Y para terminar, un caso más cercano y más conocido. Hablamos de la persona que difundió la imagen y los datos personales de la víctima de 'la Manada'. Dicha difusión la llevó a cabo en redes sociales, foros y medios digitales.

Doxing vs. DDoS

Es fácil confundirlos, porque suenan parecido, pero un ataque de doxing nada tiene que ver con un ataque DDoS.

Mientras que un ataque de doxing, como hemos visto, va dirigido hacia una víctima en concreto, con el fin de exponer su identidad y toda su

información personal en Internet. Un ataque DDoS o de denegación de servicio se dirige contra el servidor de una página web o plataforma online, con el objetivo de dejarla sin servicio, es decir, de derribarla e impedir que los usuarios puedan acceder a ella.

El doxing es o deriva en una forma de ciberacoso hacia una persona y el ataque DDoS tiene fines económicos (para extorsionar a una empresa y hacerle pagar un rescate para recuperar el servicio) o políticos."[5]

DÉCIMO PRIMERO. Hay que destacar que las apps fraudulentas ya han sido reconocidas por el Consejo Ciudadano, el cual menciona que por medio de apps ofrecen créditos o artículos como celulares y que la Ciudad de México se encuentra en primer lugar donde se cometen estos fraudes, estas malas prácticas han crecido tanto que se anuncian por televisión y redes sociales, lo cual les facilita seguir cometiendo este delito por la gran difusión que tienen; así que, las aplicaciones que siguen cometiendo fraudes no solo llegan a difundir datos o intimidar a la persona, el problema real ya se encuentra en las televisoras donde es más fácil que las personas caigan en el engaño, así como lo muestra el siguiente artículo realizado por el "Financiero" del día 25 de enero de 2021:

"Alerta ante empresas y apps fraudulentas

La semana el Consejo Ciudadano alertó sobre los más de dos mil 200 fraudes y 'doxing' en préstamos por apps que habían detectado.

Se anuncian igual en televisión, en redes sociales, en folletos a las salidas del Metro, en correos electrónicos, en medios impresos, en fin, es posible verlos en muchos lados ofreciendo créditos sin revisar Buró de Crédito, sin aval, que se otorgan de forma casi inmediata solo con llamar y mínimos requisitos, otros más solo con su perfil de Facebook o bajando a su celular una aplicación de la 'empresa' en cuestión es posible "obtener un crédito"; casi todos, por no decir todos, terminan en fraude.

La semana pasada vimos la alerta por parte del Consejo Ciudadano que preside Salvador Guerrero, sobre los más de dos mil 200 fraudes y doxing en préstamos por apps que habían detectado, en donde 64 por

[5] https://protecciondatos-lopd.com/empresas/doxing-doxeo/

ciento de las víctimas son mujeres entre 20 y 40 años, la mayoría de la CDMX, seguido del Estado de México, Veracruz, Puebla, Jalisco o Tabasco.

El análisis identifica a 130 supuestas financieras, de las que pocos medios pusieron su nombre, pero que el Consejo Ciudadano las tiene enlistadas en su página oficial. Aquí el nombre de algunas: Envía Dinero, Listo Efectivo, Cash Money, Peso Préstamo, José Cash, Cash Box, Adquiere Peso, Peso X, Crédito Lana, Presta-Club, Credit Cash, Crédito Box, Bancredi, Viva Crédito, Cash Plus, Crédito Hoy, Cash Móvil, Easy Credit,

Credit Mex, Justo Crédito, Creditya, Ifectivo, Tepresto, Lana Plus, Max Lana, Daddycredit, Good Préstamo, Dineria.mx. Todas con aplicaciones o páginas que hacen creer a las personas que son reales, o con una letra distinta a instituciones acreditadas por las que se hacen pasar, hechos que la Condusef denuncia.

Ahora bien, ya hechas las denuncias, ya sabiendo qué hacen, quiénes son y en muchas de ellas con cuentas bancarias identificadas, ¿se ha dado el siguiente paso por parte de las autoridades financieras del país?, ¿por parte de los bancos que abrieron esas cuentas? Ese es un camino que falta por recorrer y del que platicaremos el jueves, así como de los fraudes como los préstamos donde solo verifican el perfil de Facebook y que ya tienen a varias personas en el Buró de Crédito y también de empresas fraudulentas que se anuncian en los principales canales de televisión.

* * *

Y en el otro lado de la moneda, en HSBC siguen los cambios en su consejo de administración, luego de que desde inicios de año Jorge Arce fuera designado presidente y director general del grupo y del banco.

También se integraron nuevos consejeros a la institución como José María Zas, quien es expresidente y director de American Express México, Argentina y Latinoamérica y ahora también está en la Fintech Mendel; Pedro José Moreno, exvicepresidente de administración y finanzas de Santander y fundador y director general de Hill House Capital; Alberto Ardura, exdirector de operaciones de Merrill Lynch en México y director de mercados de capital en Latinoamérica de Deutsche Bank; y Andrés

Eugenio Sucre, fundador y director general de Reservamos, sitio online de compra-venta de boletos de transporte terrestre y aéreo para pasajeros en México.

En las subsidiarias del Grupo Financiero HSBC como son la Casa de Bolsa, Global Asset Management, Seguros y Pensiones se integraron como consejeros independientes Lorena Cárdenas, directora de finanzas de Abilia, compañía de bienes raíces y miembro independiente del consejo de administración de Grupo Industrial Saltillo y Eduardo Donnelly, director regional de Uber Eats Latinoamérica y exvicepresidente de servicios de seguros en American Express. Por cierto, Arce hoy tiene su primer encuentro con medios con su nuevo cargo ya que presentará el producto 'Mujeres al mundo', un crédito empresarial para el sector. Por lo pronto, la moneda está en el aire."[6]

DÉCIMO SEGUNDO. Para finalizar, La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) arroja datos concretos de las empresas fraudulentas que operan en la Ciudad de México, donde los usuarios han perdido de 10 mil hasta 100 mil pesos por estas apps engañosas, valiéndose de los datos personales de las personas, por medio de llamadas telefónicas, WhatsApp o por Facebook a través de Messenger, las apps que ofrecen créditos le piden a la o el usuario a realizar una cantidad específica en el banco, al no tener respuesta después de realizar el pago se dan cuenta que han sido defraudadas; si las autoridades ya tienen cifras y denuncias a cauda de este delito es importante y urgente que lleven a cabo mecanismos para combatir este tipo de actividades ilícitas que afectan el patrimonio de las personas.

A continuación se agregan datos emitidos en la página de La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) de lo antes mencionado:

[6] El Financiero. (25 de enero 2022).

"Alerta CONDUSEF sobre supuestas empresas que hacen uso fraudulento y suplantación del nombre de 4 entidades financieras, en la Ciudad de México

- *En este caso de 4 Sociedades Financieras de Objeto Múltiple, Entidades No Reguladas (SOFOMES, E.N.R.).*

- *Si te piden dinero antes de darte un crédito, cuidado, puedes perder tu dinero y quedarte sin el crédito solicitado.*

Ante la recurrente práctica de suplantar la identidad de entidades financieras para defraudar a las personas que buscan contratar un crédito, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), alerta de nueva cuenta a la población en general de la existencia de empresas ficticias que se ostentan como entidades financieras a través de las redes sociales, páginas de Internet apócrifas o anuncios en periódicos, las cuales ofertan supuestos créditos a cambio de cantidades de dinero que deben pagarse anticipadamente por concepto de comisiones por apertura y/o fianza.

En estos casos, las personas engañadas han pagado y perdido cantidades que van entre los mil hasta cien mil pesos, por lo que han tenido que recurrir ante el Ministerio Público a presentar la denuncia correspondiente.

En las últimas semanas, 4 Sociedades Financieras de Objeto Múltiple, Entidades No Reguladas (SOFOMES, E.N.R.) que están debidamente inscritas en el Sistema de Registro de Prestadores de Servicios Financieros (SIPRES) denunciaron ante esta Comisión Nacional el uso fraudulento y suplantación de su nombre comercial e incluso algunos de sus datos fiscales o administrativos, con los cuales defraudan a personas que buscan obtener un crédito "rápido" y "barato".

El Modus operandi de las empresas falsas usualmente es el siguiente:

1. *Utilizan información como razón social, direcciones, teléfonos e imagen corporativa (logotipos) de las Entidades Financieras debidamente*

registradas y supervisadas, para hacerse pasar por ellas. Dicha información es utilizada en documentos, contratos, publicidad, redes sociales, páginas de Internet apócrifas o anuncios en periódicos.

2. *Ofertan créditos inmediatos y con pocos requisitos, pero solicitan anticipos de dinero en efectivo o mediante depósito a una cuenta bancaria con la finalidad de apartar el crédito, gestionarlo, adelantar mensualidades, pagar gastos por apertura o como fianza en garantía, generalmente por el equivalente al 10% del monto total del crédito solicitado.*

3. *La población ha denunciado que personas que laboran en las empresas falsas los contactan vía telefónica o por redes sociales ofreciéndoles créditos con mensualidad de montos pequeños para hacerlos atractivos, sin embargo, cuando no reciben el crédito y ya pagaron los gastos exigidos, ya no los pueden localizar, o bien descubren que no trabajan para la Entidad Financiera que fue supuestamente suplantada.*

4. *Solicitan a sus víctimas enviar su información personal vía WhatsApp o por Facebook a través de Messenger, poniendo en riesgo los datos personales del público.*

NNS
HB

5. *Cuando las víctimas realizan los depósitos a la cuenta bancaria o, en algunos casos, por medio de alguna tienda de conveniencia para obtener el supuesto crédito, buscan contactar a la entidad falsa y al no tener respuesta, recurren a la CONDUSEF para verificar su existencia y es cuando descubren que han sido víctimas de un supuesto fraude.*

Por lo anterior y a fin de evitar que seas sorprendido por este tipo de prácticas de fraude y suplantación de Entidades Financieras, la CONDUSEF te recomienda que antes de solicitar algún tipo de crédito, tomes en cuenta lo siguiente:

- *Evita contratar préstamos o créditos en los que tengas que dar anticipos.*
- *Asegúrate que la Institución o Entidad Financiera esté registrada ante el SIPRES que administra la CONDUSEF; puedes llamarnos para verificar su domicilio, página de internet y teléfonos. https://webapps.condusef.gob.mx/SIPRES/jsp/pub/index.jsp*
- *No proporciones dinero antes del otorgamiento de un crédito, ya sea por concepto de seguro, comisión o gestión del crédito.*

- *No entregues documentos personales o datos de tarjetas de crédito o débito.*
- *No des información ni realices operaciones a través de Facebook, WhatsApp, o cualquier otra red social si no investigaste que se trata de una entidad financiera.*
- *Asegúrate que las personas con las que contactas realmente laboren en la entidad financiera.*
- *No firmes ningún documento antes de leerlo completa y detalladamente.*
- *En caso de que la razón social contenga las siglas S.A. de C.V., asegúrate que esa empresa o entidad realmente exista. Puedes consultar su domicilio, página de internet y teléfonos ante la PROFECO o la CONDUSEF.*
- *Si utilizas Internet como medio de contacto, asegúrate de verificar la información.*

NNS
HB

A continuación, te damos a conocer a las SOFOMES, E.N.R., debidamente registradas ante la CONDUSEF, cuya identidad ha sido suplantada:

No.	Entidad financiera debidamente registrada en la CONDUSEF	"Empresa" suplantadora y/o falsa	Lugar y/o medio
1	Crédito Único, S.A. de C.V. SOFOM, E.N.R.	Crédito Único. **(Utiliza la misma razón social, por lo que se debe verificar ante la CONDUSEF la correcta).**	CDMX, a través de las redes sociales Facebook y WhatsApp.
2	Financiamiento Progresemos, S.A. de C.V., SOFOM, E.N.R.	PROGRE$EMOS, S.A. de C.V. **(Utiliza la misma razón social, por lo que se debe verificar ante la CONDUSEF la correcta).**	CDMX, a través de correos electrónicos y la red social WhatsApp.
3	Baracaf, S.A. de C.V., SOFOM, E.N.R.	Servicios Financieros CREAFI. **(Utiliza la misma razón social, por lo que se debe verificar ante la CONDUSEF la correcta).**	CDMX, a través de la red social Facebook.
4	Siempre Creciendo, S.A. de C.V., SOFOM, E.N.R.	Creciendo al Mundo. **(Utiliza la misma razón social, por lo que se debe verificar ante la CONDUSEF la correcta).**	CDMX, a través de página web, correos electrónicos y las redes sociales Facebook y WhatsApp.

[7] https://www.condusef.gob.mx/?p=contenido&idc=1301&idcat=1

PROPOSICIÓN CON PUNTO DE ACUERDO POR LA CUAL SE EXHORTA A LA POLICÍA CIBERNÉTICA DE LA SECRETARÍA DE SEGURIDAD CIUDADANA DE LA CIUDAD DE MÉXICO, INVESTIGUE A LAS 130 APPS QUE DEFRAUDAN Y EMPLEAN COBRANZA ILEGITIMA A TRAVÉS DE DIFUNDIR LA DEUDA, Y EN ALGUNOS CASOS FOTOS O VÍDEOS, ENTRE SUS CONTACTOS, VIOLENTANDO LA PROTECCIÓN DE LOS DATOS PERSONALES DE LOS CIUDADANOS

V. PUNTOS RESOLUTIVOS

Por lo anteriormente expuesto y fundado, en términos de los razonamientos de hecho y de derecho, y de conformidad con lo establecido en los artículos 103 y 104 del Reglamento del Congreso de la Ciudad de México, esta Comisión Dictaminadora:

RESUELVE

ÚNICO. Se **aprueba** la proposición con punto de acuerdo por la cual se exhorta a la policía cibernética de la secretaría de seguridad ciudadana de la ciudad de México, investigar las 130 apps que defraudan y emplean cobranza ilegitima a través de difundir la deuda, y en algunos casos fotos o videos, entre sus contactos, violentando la protección de los datos personales de los ciudadanos, que presentó el Diputado José Gonzalo Espina Miranda, integrante del Grupo Parlamentario del Partido Acción Nacional.

LISTA DE VOTACIÓN DE LA COMISIÓN DE SEGURIDAD CIUDADANA

DIPUTADO (A)	A FAVOR	EN CONTRA	ABSTENCIÓN
 DIP. NAZARIO NORBERTO SÁNCHEZ **PRESIDENTE**	Nazario Norberto Sánchez		

Doc ID: 0390da8d488291eccd633813a852a6a4bcad5218

	DIP. MARÍA DE LOURDES GONZÁLEZ HERNÁNDEZ **VICEPRESIDENTA**			
	DIP. HÉCTOR BARRERA MARMOLEJO **SECRETARIO**	Hector Barrera		
	DIP. ALICIA MEDINA HERNÁNDEZ **INTEGRANTE**	Dip. Alicia Medina Hernández		
	DIP. ANÍBAL ALEXANDRO CAÑEZ MORALES **INTEGRANTE**			
	DIP. BLANCA ELIZABETH SÁNCHEZ GONZÁLEZ **INTEGRANTE**	Elizabeth Sánchez		

	DIP. CARLOS CERVANTES GODOY **INTEGRANTE**			
	DIP. DIANA LAURA SERRALDE CRUZ **INTEGRANTE**			
	DIP. FAUSTO MANUEL ZAMORANO ESPARZA **INTEGRANTE**	Fausto Zamorano Esparza		
	DIP. JORGE GAVIÑO AMBRIZ **INTEGRANTE**			
	DIP. JOSÉ GONZALO ESPINA MIRANDA **INTEGRANTE**	Gonzalo Espina Miranda		

	DIP. JOSÉ MARTÍN PADILLA SÁNCHEZ **INTEGRANTE**			
	DIP. LUIS ALBERTO CHÁVEZ GARCÍA **INTEGRANTE**	Luis Chávez		
	DIP. RICARDO JANECARLO LOZANO REYNOSO **INTEGRANTE**			
	DIP. SANDY HERNÁNDEZ MERCADO **INTEGRANTE**	Sandy Hernández Mercado		

Dado en el Congreso de la Ciudad de México, el 1 de abril del mes de abril del 2022.