DIP. HÉCTOR DÍAZ POLANCO, PRESIDENTE DE LA MESA DIRECTIVA DEL CONGRESO DE LA CIUDAD DE MÉXICO, II LEGISLATURA.

PRESENTE

Honorable Congreso de la Ciudad de México.

El que suscribe Diputado **Nazario Norberto Sánchez**, integrante del Grupo Parlamentario de MORENA del Congreso de la Ciudad de México, II Legislatura, con fundamento en los artículos 122 apartado A, fracciones I y II párrafo 5 de la Constitución Política de los Estados Unidos Mexicanos; 29 Apartado D, inciso a) y 30 numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 12 fracción II, y 13 párrafo primero de la Ley Orgánica del Congreso de la Ciudad de México; 5 fracciones I y II, 82, 95 fracción II, 96 Reglamento del Congreso de la Ciudad de México, someto a consideración de este Pleno la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL CAPÍTULO III, AL TÍTULO DÉCIMO SÉPTIMO DEL CÓDIGO PENAL PARA LA CIUDAD DE MÉXICO, EN MATERIA DE CIBERDELITOS O DELITOS INFORMÁTICOS,** al tenor de las consideraciones siguientes:

I. Planteamiento del problema que se pretende resolver.

El desarrollo tecnológico, la interdependencia económica, la desmedida informatización de la sociedad y el absoluto poder de la Informática, han demandado al Derecho Penal la comprensión de las conductas en las que se ve inmersa la informática o bien todo medio electrónico, lo anterior en atención de las acciones propias del hombre resultado de una situación principalmente socioeconómica, antropológica y psíquica que requiere desde luego un tratamiento jurídico específico.

De acuerdo con el texto, los delitos informáticos de la Universidad Nacional Autónoma de México[1], este tipo de delitos son definidos como *"…actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".* Asimismo, se menciona en el mismo texto que, de acuerdo con el autor Carlos Sarzana, los delitos informáticos son *"…cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo…"*[2]

Algunos de las principales características de los delitos informáticos son las siguientes, de acuerdo a la doctrina:

a) *"… son conductas criminógenas de cuello blanco (White collar cirmes), en tanto que solo determinado número de personas con ciertos conocimientos (en este casi técnicos), pueden llegar a cometerlas;*
b) *Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando;*
c) *Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico;*
d) *Provocan serias pérdidas económicas ya que casi siempre producen beneficios de más de 5 cifras a aquellos que los realizan;*
e) *Ofrecen facilidades de tiempo y espacio ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse;*

[1] https://archivos.juridicas.unam.mx/www/bjv/libros/4/1941/16.pdf
[2] Ibidem.

f) Son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de regulación por parte del derecho;

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar;

h) Presentan grandes dificultades para su comprobación esto por su mismo carácter técnico.

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención

j) Ofrecen facilidades para su comisión a los menores de edad

k) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley…"

En la actualidad ya se han manifestado diversos delitos que han tenido relación íntima con las tecnologías de la información, delitos que se incrementan año con año debido a que la realidad ha superado la propia legislación en esta materia, por ejemplo, mundialmente se han reconocido conductas criminales de cuello blanco algunas destacadas por los siguientes nombres:

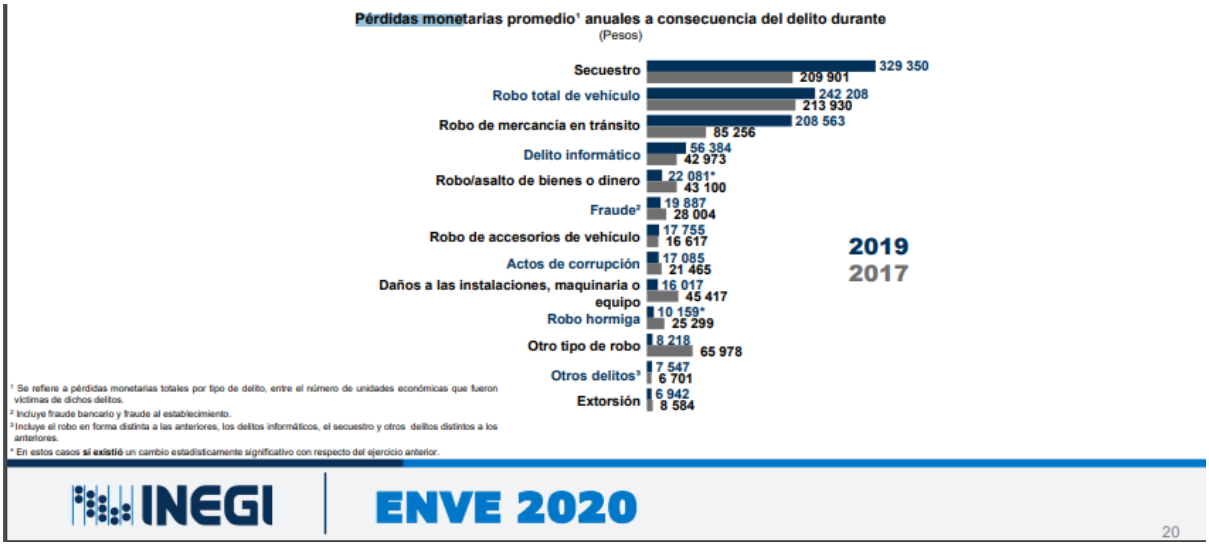
- hacking,
- cracking,
- phishing,
- evil twins,
- pharming y spamming;
- robo de identidad;
- ciberterrorismo;
- propagación de Malware, a través de las redes de datos;
- el empleo de tecnologías pop-up ads y adware, la instalación de sniffers, spyware, o programas espía en las computadoras personales para conocer los hábitos y actividades de familiares o empleados;

así como la vigilancia internacional de las comunicaciones electrónicas a través de programas gubernamentales como ECHELON o los de control fronterizo como el USVISIT, son tan sólo algunas de las tantas expresiones de tan variada fenomenología que han hecho que la seguridad jurídica de las personas y de las transacciones comerciales electrónicas, dependan de las medidas de seguridad de los sistemas informáticos de información y comunicación.

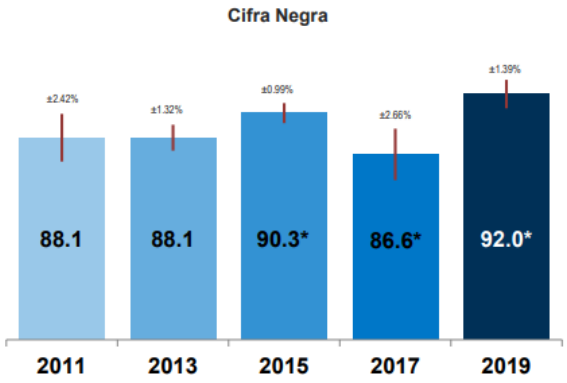
Lo anterior evidencia que a cada paso de avance en la tecnología es un avance en la posibilidad de hacer un uso inadecuado de ella para dañar a las personas, lo cual desde luego demanda a nivel mundial la actualización de los marcos jurídicos a fin de que se construya un andamiaje legal que haga frente al mal uso de la informática, principalmente en materia penal.

En nuestro país, de acuerdo con la encuesta Nacional de Victimización de empresas (ENVE 2020)[3], que permite complementar la información sobre victimización a nivel nacional, conjuntamente con la victimización en hogares, a través de la Encuesta Nacional de victimización y percepción sobre seguridad pública (ENVIPE), señala que en 2019, la pérdida monetaria por victimización en unidades económicas, esto es, aquellas pérdidas a consecuencia de haber sido víctima de uno o más delitos, ascendido a 225.9 mil millones de pesos, de lo cual los **delitos informáticos** pasaron a ser la cuarta causa de éstas pérdidas, como se muestra a continuación:

[3] https://www.inegi.org.mx/contenidos/programas/enve/2020/doc/enve_2020_presentacion_ejecutiva.pdf



Asimismo, a nivel nacional se señala que la cifra negra fue mayor en el caso de actos de corrupción y el delito de extorsión durante el año 2019, encontrándose los **delitos informáticos** en el sexto lugar, como se muestra a continuación:



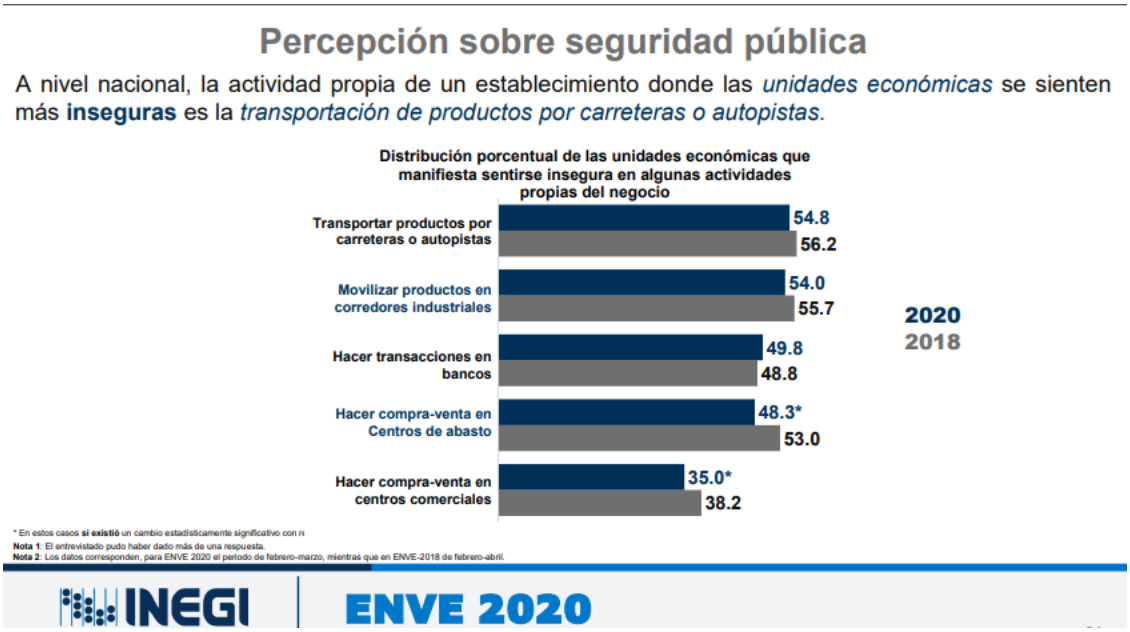
Cifra Negra (%)		
Tipo de delito	2017	2019
Actos de corrupción	99.1	99.7
Extorsión	97.4	98.7*
Fraude	95.4	97.6
Robo hormiga	94.4	95.5
Secuestro	92.1	94.9
Delito informático	95.3	94.8
Daños a las instalaciones, maquinaria o equipo	91.5	91.7
Robo parcial de vehículo	95.1	91.1
Robo/asalto de bienes o dinero	72.5	88.5*
Otro tipo de robo¹	66.4	77.5
Robo de mercancía en tránsito	70.3	76.3
Robo total de vehículo	9.1	23.0*

¹ Se refiere a robos distintos de robo o asalto de mercancía, dinero, insumos o bienes, robo total o parcial de vehículo, robo de mercancía en tránsito y robo hormiga.
* En estos casos sí existió un cambio estadísticamente significativo con respecto del ejercicio anterior.

INEGI ENVE 2020 26

También con relación a la percepción sobre la inseguridad pública, a nivel nacional la actividad propia de un establecimiento donde las unidades económicas se sienten

más inseguras en primer lugar es la transportación de productos por carreteras y autopistas, sin embargo, las transacciones en bancos han quedado en tercer lugar como se evidencia a continuación:



Por otro lado, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, expone que al segundo trimestre de 2021, las quejas por fraudes cibernéticos disminuyeron en 5.0% respecto de 2020 y representan cada año una mayor proporción, al pasar de 47% en 2017 al 70% en 2021[4]:

	2017	2018	2019	2020	2021	VAR. (2021 vs 2020)
TOTALES	3,345,664	3,515,712	4,318,853	4,303,006	3,948,443	
CIBERNÉTICOS	1,578,000	2,074,554	2,807,819	2,889,730	2,745,738	-5.0%
	47%	59%	65%	67%	70%	-
TRADICIONALES	1,762,805	1,441,115	1,511,022	1,413,276	1,202,705	-14.9%
	53%	41%	35%	33%	30%	-
Por definir	4,859	43	12	0	0	-

[4] https://www.condusef.gob.mx/?p=estadisticas

Tabla 1. Elaborada por CONDUSEF Fraudes Cibernéticos y Tradicionales

Sin embargo, el monto reclamado de los fraudes cibernéticos ascendió a $6,532 millones de pesos; se bonificó sólo el 41% y 84 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario:

Al segundo trimestre 2021						
	Reclamaciones Iniciadas	Monto Reclamado (mdp)	Monto Reclamado Concluido (mdp)	Monto Abonado (mdp)	% de abono	% de resolución Favorable
TOTAL DE FRAUDES	**3,948,443**	**$10,841**	**$9,899**	**$3,525**	**36**	**74**
Comercio por Internet	2,534,130	$2,973	$2,818	$2,205	78	91
Banca Móvil	119,179	$1,191	$1,076	$40	4	2
Operaciones por Internet P. Físicas	89,324	$1,968	$1,667	$175	11	16
Operaciones por Internet P. Morales	3,076	$400	$332	$25	8	6
Pagos por Celular	29	$0	$0	$0	0	0
SUBTOTAL CIBERNÉTICO	**2,745,738**	**$6,532**	**$5,893**	**$2,446**	**41**	**84**
Terminal Punto de Venta	766,797	$1,695	$1,567	$497	32	45
Comercio por Teléfono	258,461	$385	$306	$205	67	81
Cajeros Automáticos	96,184	$403	$384	$53	14	10
Sucursales	79,726	$1,717	$1,648	$299	18	19
Corresponsales	467	$2	$2	$1.3	78	70
Movimiento generado por el Banco	386	$46	$44	$9	20	37
Otros Bancos	364	$18	$16	$4	25	31
Banca por Teléfono	320	$44	$38	$12	31	46
SUBTOTAL TRADICIONAL	**1,202,705**	**$4,310**	**$4,005**	**$1,080**	**27**	**47**
Por Definir	-	-	-	-		-

Tabla 2. Elaborada por CONDUSEF Fraudes Cibernéticos y Tradicionales

Empero, ello no significa que los fraudes financieros realmente se sancionen de acuerdo a la legislación penal.

Aunado a lo anterior, cabe señalar que los delitos informáticos desgraciadamente se incrementaron un 20% derivado de la pandemia por COVID 19, debido principalmente al uso preponderante de medios electrónicos para realizar transacciones bancarias o compras, al respecto se cita la siguiente nota periodística:

*"…**Los ataques cibernéticos aumentan un 40% en México durante la pandemia***
19 noviembre, 2020

El ciberdelito en tiempos de Covid en México.
El nuevo coronavirus llegó para cambiar intempestivamente nuestras formas de vida: las medidas de confinamiento, el uso universal de mascarillas, la migración hacia el teletrabajo, todo ha experimentado un giro en lo que se ha dado en llamar la nueva normalidad. Esa nueva normalidad ha sido también una oportunidad para delincuentes informáticos para incrementar exponencialmente los ataques a través de la tecnología digital.

La presencia que ya tenía el uso del internet es nuestra vida cotidiana experimentó un impulso nunca antes visto: comprar, comunicarnos, divertirnos, trabajar: todo o casi todo se ha hecho por internet desde el primer trimestre del año 2020. Según estimaciones el comercio electrónico creció alrededor de 108 % a nivel global, mientras que el uso de herramientas digitales se duplicó en tan solo los dos primeros meses de la pandemia.

En el caso de México, la facturación de las tiendas en línea se ha incrementado en un 60%, cifra que resulta imponente teniendo en cuenta que la penetración del internet no es tan elevada como países europeos o EE. UU.

Ahora bien, el crecimiento de estas estadísticas ha ocasionado también un incremento alarmante de las amenazas cibernéticas. Para el último trimestre del 2020 se considera que existen un 75 % más de probabilidades de ser víctimas de un ciberdelito en comparación con el 2019. Además, con el 22 % de todos los ataques, México ocupa el segundo lugar de todos los delitos informáticos cometidos en la región, solo después de Brasil.

¿Estamos ante una ciberpandemia?

Algo que es más alarmante es la diversificación de las técnicas de los hackers para cometer sus fechorías, pues según BTR Consulting durante el tiempo de Covid se ha detectado más de 130 nueva modalidades de ataques informáticos. A continuación te contamos cuáles han sido los delitos cibernéticos más comunes durante 2020:

1. El ransomware no descansa

Según un informe actualizado de Kaspersky enfocado en América Latina, es una de las empresas de ciberseguridad más importantes a nivel mundial, ya que en el continente se ha detectado un promedio de 5 mil ataques de ransomware diariamente y México ocupa el segundo lugar de la lista. Una de las causas del ascenso en el uso de este malware de rescate se debe al aprovechamiento de la vulnerabilidad que genera el uso de aplicaciones informáticas que no cuenta con la debida actualización.

2. Fraude en banca en línea

Como era de esperarse, el uso de las plataformas digital de los bancos también creció exponencialmente durante este periodo. Por ello, los piratas informáticos dedicaron buena parte de sus esfuerzos a crear software maliciosos para robar los datos bancarios.

Este tipo de acciones es tal vez la más sencilla de realizar, puesto que las personas dejan "huellas" que le permiten a los delincuentes rastrear y apropiarse de credenciales bancarias. La proliferación de estos códigos maliciosos superó el 550 % en relación con el 2019.

3. Compras online fraudulentas

Las condiciones de angustia que generó la crisis sanitaria tanto por el confinamiento como por los desequilibrios en la economía de las familias, se convirtió en una oportunidad para estafar a través de las compras electrónicas. Desde falsas oportunidades de trabajo en casa, el ofrecimiento de vacunas anticovid, hasta ofertas irresistibles en productos muy demandados, fueron muchas las formas de engañar a las personas para adueñarse de su dinero o de información confidencial. El modus operandi más común fue la creación de clones de páginas de tiendas o empresas reconocidas, incluso campañas de phishing.

4. Ataques a infraestructuras críticas

Afectar el funcionamiento de servicios esenciales para la sociedad durante el tiempo de crisis, ha sido otra práctica bastante común y muy rentable para los hackers. Sin importar los problemas colectivos que puedan ocasionar, han perfeccionado las estrategias para violentar la seguridad de los servidores o aprovechar las vulnerabilidades de los software.

¿Por qué se han incrementado las ciberamenazas durante 2020?

No podemos terminar este post sin mencionar las razones por las que este fenómeno ha crecido tanto durante los últimos meses. La causa principal no

radica en el aumento del uso de los canales electrónicos para realizar distintas actividades cotidianas, sino en la poca educación en seguridad cibernética que tienen las personas y las pocas medidas de seguridad informática que implementan las organizaciones.

Un altísimo porcentaje de las amenazas pueden ser neutralizadas con las aplicaciones de protocolos de ciberseguridad por parte de los usuarios de internet, con la actualización oportuna de software, con la utilización de programas dotados con protocolos seguros y con la instalación de herramientas de ciberseguridad electrónica.

En medio de la crisis sanitaria el mundo enfrenta también una crisis cibernética. De todos depende superarla o ser víctimas de ella….”[5]

Asimismo, es imperativo señalar que no solamente el fraude, el robo o la extorsión son delitos que se han realizado a través de medios tecnológicos sino también existen delitos a través de los medios informáticos que atentan en contra de niñas, niños y adolescentes a través de las redes sociales.

Al respecto, la Policía cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México, ha registrado en este año 2021 un mayor incremento de delitos como el acoso, sexting, grooming, ciberbullyng, difusión de contenidos sexuales sin consentimiento y pornografía infantil.

De acuerdo con información del periódico El Universal[6], Elizabeth Melchor, especialista y policía adscrita a la unidad de la Policía Cibernética, explicó que este tipo de delitos han registrado mayor incidencia entre este sector de la sociedad,

[5] https://fractaliasystems.com/los-ataques-ciberneticos-aumentan-40-en-mexico-durante-la-pandemia/
[6] https://www.eluniversal.com.mx/metropoli/aumentan-ciberdelitos-contra-menores-por-pandemia-usan-mas-internet

debido a que la pandemia por Covid-19 hizo que muchos migraran sus actividades escolares a internet.

La especialista dijo que con esta modalidad muchos de los ciberdelincuentes han encontrado la manera de iniciar un ciclo de persuasión con niñas, niños y adolescentes para obtener información y utilizarla para chantajes, extorsión, amenazas, y en algunos casos, concretar diversos encuentros físicos, al respecto se cita la siguiente nota:

> *"**Aumentan ciberdelitos contra menores: por pandemia, usan más internet***
> *11/10/2021*
> *Kevin Ruiz*
> *Son víctimas de acoso, grooming, ciberbullying, entre otros, pues por pandemia usan más internet; son 5% de los reportes al mes, dice*
> *…*
> *…*
> *…*
> *…**facebook, Instagram, Tik Tok** y juegos en línea son las principales plataformas donde los menores de edad están en riesgo de ser víctimas de un delito, comentó la uniformada en entrevista con **EL UNIVERSAL**.*
>
> *"Todo comienza con un ciclo en el que los delincuentes se ganan la confianza de los menores y adolescentes a través de cuentas o perfiles falsos, en donde terminan incitándolos a enviar fotografías con contenido sexual o de diferente índole, que inevitablemente termina en la comisión del delito de pornografía infantil.*
>
> *"Un 1% o 2% corresponde a pornografía infantil. [En] la pornografía infantil hay que tener en cuenta que engloba hasta el acoso a menores, sexting, grooming, pero es importante resaltarlo", comentó.*
>
> *Antes se podían encontrar grupos de Facebook además de otros espacios como páginas web, los cuales eran de fácil ubicación para las autoridades; sin embargo, ahora hay puertas de entrada en redes sociales como Telegram y WhatsApp, donde las cadenas son más grandes.*

Melchor reconoció que hay un catálogo amplio de otros delitos que se pueden desencadenar, como secuestro, trata de personas y obligar a los menores a la venta de drogas.
*"El **catálogo [de delitos] es amplio**, lamentablemente; sin embargo, lo que hace esta unidad para alertar a los niños y adolescentes, pero principalmente a los padres, madres y tutores, es a través de **alertas preventivas** y pláticas, informar sobre cómo se puede prevenir", expuso.*

Independientemente de las alertas que realizan, detalló que han recortado los tiempos de respuesta ante un caso y, además, la policía capitalina ha sido requerida más veces a través de mandamientos ministeriales para hacer cualquier tipo de búsqueda o que se comparta información para investigaciones, pero no precisó el número de estos requerimientos.

Caída de redes
La policía Elizabeth Melchor aseguró que con la caída de las redes sociales el pasado lunes, los usuarios no están en riesgo de perder información o que sea utilizada para la comisión de delitos.

*El lunes, cuando se registró un apagón en las redes, la policía realizó un monitoreo y no registraron reportes de **incidencia delictiva** de ningún tipo, tampoco, reportes de usuarios.*

"El robo de información [puede suceder] haya o no un apagón [de redes], puede darse en cualquier momento a través de una cadena, un sitio falso", dijo…"

Es menester señalar que el Gobierno de México, y desde luego el Gobierno de la Ciudad de México han encaminado acciones en materia de prevención del delito en cuestiones informáticas, por ejemplo, el pasado 25 de octubre del año en curso se llevó a cabo la séptima semana de ciber seguridad de la Guardia Nacional para prevenir y combatir los ciberdelitos con énfasis en la problemática que padecen niñas, niños y adolescentes en el contexto de la pandemia, la infodemia y su impacto emocional.

Durante dicho evento, la titular de la Secretaría de Seguridad y Protección Ciudadana (SSPC), Rosa Icela Rodríguez Velázquez, presentó una Ciberguía para prevenir delitos y violencia digital[7], donde se ofrecen recomendaciones básicas sobre el uso adecuado de Internet y redes sociales. Asimismo, aclaró que no se trata de satanizar a la tecnología, sino de hacer un uso adecuado de ella e invitó a padres de familia y maestros a consultar el documento, así como el Decálogo para el uso de videojuegos[8], presentado recientemente.

Bajo ese orden de ideas, es importante señalar un gran avance que se tuvo en el Congreso de la Ciudad de México, en conjunto con la Jefatura de Gobierno, puesto que en la Primera Legislatura aprobamos en la Comisión de Administración y Procuración de Justicia y posteriormente en el Pleno, la Ley Olimpia contra el acoso digital que impone penas de hasta seis años por difundir imágenes de contenido íntimo y sexual sin el consentimiento de la persona implicada.

No obstante, el avance la tecnología cada vez está superando a la propia legislación tradicional, por lo que es necesario que la misma sea actualizada conforme a las demandas de la propia sociedad, quien cada día es o puede ser víctima de estos delitos a través de los sistemas de cómputo o electrónicos, principalmente las y los menores de 18 años de edad, quienes son los primeros que acceden a una computadora.

Es menester señalar que el estado de Sinaloa, fue el primero que cronológicamente tipificó el delito informático y el que también lo denomina de esa forma en su Código

[7] https://www.gob.mx/cms/uploads/attachment/file/676826/Ciberguia_completa_1.0_alta-compressed.pdf
[8] https://presidente.gob.mx/presentan-decalogo-para-la-seguridad-de-menores-de-edad-en-internet-presidente-alerta-sobre-contenido-danino-de-videojuegos/

Penal, seguido de algunos estados como Jalisco, Nuevo León y Quintana Roo, para el caso de delitos específicos.

Por lo que hace a la Ciudad de México, en la V Legislatura de la Asamblea Legislativa del Distrito Federal, se presentó una iniciativa que atendía también esta problemática, sin embargo, no fue realizado el dictamen respectivo que la atendía.

Respecto al Código Penal Federal, es menester señalar que se encuentra tipificado el *"acceso ilícito a sistemas y equipos de informática",* y el uso de los sistemas de cómputo para el delito de *"Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo."*

De tal suerte, la Ciudad de México no debe de ser la excepción al atender urgentemente esta problemática, la cual año con año se actualiza para afectar a más empresas públicas y privadas y por supuesto a las personas que utilizamos a diario los medios o dispositivos electrónicos.

II. Propuesta de Solución.

En ese sentido, se realiza la presente Iniciativa con Proyecto de Decreto por el que se adiciona el capítulo III al Título Décimo Sétimo del Código Penal de la Ciudad de México, con el propósito de establecer una penalidad de 3 a 5 años de prisión y de 300 a 500 unidades de medida y actualización a quien haga uso indebido de las tecnologías de la información y comunicación para defraudar, obtener dinero, bienes o información; o provoque la pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; así como a quien modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado o de empresas privadas, protegidos

por algún mecanismo de seguridad, y finalmente, se agrava la pena hasta una tercera parte cuando la información sea utilizada en provecho propio o ajeno, se cometa por algún servidor público o bien, se aumentará hasta en una mitad cuando a través del uso de los medios electrónicos o informáticos y redes sociales, se realicen conductas de usurpación de identidad, abuso y acoso sexual, fraude, extorsión o cualquier otro hecho que la ley señale como delito. En ese sentido, la propuesta quedaría de la siguiente manera:

DICE	DEBE DECIR
TÍTULO DÉCIMO SÉPTIMO **DELITOS CONTRA LA SEGURIDAD COLECTIVA** **CAPÍTULO I.** **PORTACIÓN, FABRICACIÓN E IMPORTACIÓN DE OBJETOS APTOS PARA AGREDIR.** **…** **CAPÍTULO II.** **PANDILLA, ASOCIACIÓN DELICTUOSA Y DELINCUENCIA ORGANIZADA.** … ***(sin correlativo)***	**TÍTULO DÉCIMO SÉPTIMO** **DELITOS CONTRA LA SEGURIDAD COLECTIVA** **CAPÍTULO III.** **DELITOS INFORMÁTICOS** **Artículo 255 Bis.** Se le impondrá una pena de tres a cinco años de prisión y de trecientas a quinientas unidades de medida y actualización:

	I. Al que use o entre a una base de datos, sistema de computadoras, red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar, modificar, destruir, copiar, o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o provoque la pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad; II. Al que intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. III. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado o de empresas privadas, protegidos por algún mecanismo de seguridad. **Artículo 255 Ter.** Las penas previstas en este capítulo se aumentarán hasta en una tercera parte cuando: I. la información obtenida se utilice en provecho propio o ajeno; o II. Sean cometidas por un Servidor público, en el que además se impondrá la destitución e inhabilitación de tres a seis años para desempeñarse en otro empleo, puesto, cargo o comisión.

	Artículo 255 Quáter. Las penas se aumentarán en hasta en una mitad cuando a través del uso de los medios electrónicos o informáticos y redes sociales, se realicen conductas de usurpación de identidad, abuso y acoso sexual, fraude, extorsión o cualquier otro hecho que la ley señale como delito.

Con base en los razonamientos antes precisados, el suscrito Diputado propone al Pleno este Congreso de la Ciudad de México, II Legislatura, la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL CAPÍTULO III, AL TÍTULO DÉCIMO SÉPTIMO DEL CÓDIGO PENAL PARA LA CIUDAD DE MÉXICO, EN MATERIA DE CIBERDELITOS O DELITOS INFORMÁTICOS,** para quedar como sigue:

D E C R E T O

ÚNICO.

TÍTULO DÉCIMO SÉPTIMO
DELITOS CONTRA LA SEGURIDAD COLECTIVA

CAPÍTULO I.

PORTACIÓN, FABRICACIÓN E IMPORTACIÓN DE OBJETOS APTOS PARA AGREDIR.

…

CAPÍTULO II.

PANDILLA, ASOCIACIÓN DELICTUOSA Y DELINCUENCIA ORGANIZADA.

…

CAPÍTULO III.
DELITOS INFORMÁTICOS

Artículo 255 Bis. Se le impondrá una pena de tres a cinco años de prisión y de trecientas a quinientas unidades de medida y actualización:

I. Al que use o entre a una base de datos, sistema de computadoras, red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar, modificar, destruir, copiar, o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o provoque la pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad;

II. Al que intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

III. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado o de empresas privadas, protegidos por algún mecanismo de seguridad.

Artículo 255 Ter. Las penas previstas en este capítulo se aumentarán hasta en una tercera parte cuando:

I. la información obtenida se utilice en provecho propio o ajeno; o

II. Sean cometidas por un Servidor público, en el que además se impondrá la destitución e inhabilitación de tres a seis años para desempeñarse en otro empleo, puesto, cargo o comisión.

Artículo 255 Quáter. Las penas se aumentarán en hasta en una mitad cuando a través del uso de los medios electrónicos o informáticos y redes sociales, se realicen conductas de usurpación de identidad, abuso y acoso sexual, fraude, extorsión o cualquier otro hecho que la ley señale como delito.

ARTÍCULOS TRANSITORIOS

PRIMERO. El presente decreto entrara en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. Remítase a la Jefatura de Gobierno para su publicación en la Gaceta Oficial de la Ciudad de México.

TERCERO. Se derogan todas las disposiciones que se opongan al presente Decreto.

Dado en el Recinto del Congreso de la Ciudad de México a los 11 días del mes de noviembre de 2021.

ATENTAMENTE

Nazario Norberto Sánchez

DIP. NAZARIO NORBERTO SÁNCHEZ

DISTRITO IV.