En la Ciudad de México, a los 11 días del mes de octubre de 2022.

DIPUTADO FAUSTO MANUEL ZAMORANO ESPARZA, PRESIDENTE DE LA MESA DIRECTIVA DEL CONGRESO DE LA CIUDAD DE MÉXICO, II LEGISLATURA.

P R E S E N T E.

Quien suscribe, **ALBERTO MARTÍNEZ URINCHO**, diputado integrante del Grupo Parlamentario de Morena en el Congreso de la Ciudad de México, II Legislatura, con fundamento en lo dispuesto por los artículos 122, Apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 29, 30, numeral 1, inciso b), de la Constitución Política de la Ciudad de México; 4° fracción XXI y 12 fracción II, de la Ley Orgánica del Congreso de la Ciudad de México; 5, fracción I, 79 fracción VI, 82, 95, fracción II, 96 y 325 del Reglamento del Congreso de la Ciudad de México, me permito presentar la siguiente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN ARTÍCULO 211. BIS. 5.1. AL CÓDIGO PENAL FEDERAL, Y QUE SE PRESENTA ANTE EL CONGRESO DE LA UNIÓN**, al tenor de lo siguiente:

I. DENOMINACIÓN DEL PROYECTO DE LEY O DECRETO.

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UN ARTÍCULO 211. BIS. 5.1. AL CÓDIGO PENAL FEDERAL, Y QUE SE PRESENTA ANTE EL CONGRESO DE LA UNIÓN.

II. OBJETIVO DE LA PROPUESTA.

Crear un nuevo tipo penal relacionado con el secuestro o uso indebido de datos personales registrados en archivos públicos o privados.

III. PLANTEAMIENTO DEL PROBLEMA QUE LA INICIATIVA PRETENDA RESOLVER Y LA SOLUCIÓN QUE SE PROPONE.

Ante el creciente número de fraudes, extorsiones y suplantación de identidad por medios digitales es importante tipificar nuevas conductas delictivas para sancionarlas.
Mejorar.

IV. ARGUMENTOS QUE LA SUSTENTAN.

PRIMERO. – La efectividad de la justicia penal es parte esencial de una estrategia de seguridad cibernética. Esto comprende la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos, al igual que la obtención de evidencia electrónica relacionada con cualquier delito, para propósitos del proceso penal.

La naturaleza transnacional del delito cibernético y en particular la volatilidad de la evidencia electrónica implica que la justicia penal no puede ser efectiva sin una cooperación internacional eficiente. La legislación integral, que incluye el derecho sustantivo (la conducta a ser definida como delito) y el derecho procesal (los poderes investigativos para la aplicación de la ley), es fundamental para que tenga lugar la respuesta de la justicia penal.

Tal legislación debe cumplir con varios requisitos:

Debe ser lo suficientemente neutral (tecnológicamente) como para responder a la evolución constante del crimen y la tecnología, ya que de no ser así corre el peligro de volverse obsoleta para cuando entre en vigor.

Los poderes para la aplicación de la ley deben estar sujetos a salvaguardias con el fin de garantizar el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos.

Debe operar con suficiente armonía o por lo menos ser compatible con las leyes de otros países para permitir la cooperación internacional; por ejemplo, el cumplimiento con la condición de la doble criminalidad.

SEGUNDO. – Ahora bien, los tipos de delitos informáticos reconocidos por Naciones Unidas[1] son los siguientes:

1. Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los datos de entrada.

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b) Manipulación de programas.

[1] Ver: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm, 6 de octubre de 2022.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) Manipulación de los datos de salida.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo.

Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas.

a) Las falsificaciones informáticas como objeto.

Cuando se alteran datos de los documentos almacenados en forma computarizada.

b) Las falsificaciones informáticas como instrumentos.

Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados.

a) sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

b) Virus.

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar

en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

c) Gusanos.

Se fábrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

d) Bomba lógica o cronológica.

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4. Acceso no autorizado a servicios y sistemas informáticos.

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

a) Piratas informáticos o hackers.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

b) Reproducción no autorizada de programas informáticos de protección legal

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

TERCERO. - La aceleración digital que vemos desde hace algunos años, se vio potenciada de manera exponencial por una pandemia que obligó a cientos de miles de usuarios a consumir cada vez más servicios y productos de manera online, y a las compañías a digitalizar procesos que previamente se realizaban de manera física.

Esta combinación de factores da sentido al nuevo apodo que los expertos en ciberseguridad han denominado como el "nuevo oro": los datos e información. Ya sea información crediticia o financiera, de salud, de accesos a cuentas, gubernamental o de un simple registro, tanto de usuarios, interna o externa, los cibercriminales la persiguen con finalidad de conseguir una ganancia monetaria. Esta se obtiene mediante la venta de la información robada en mercados negros, la extorsión a las víctimas para no revelar la información o la ejecución de otros ataques usando los datos.

No es de extrañar, entonces, que existan amenazas diseñas específicamente para el robo de datos y el espionaje, denominadas Spyware. En esta categoría encontramos a los *keyloggers,* RAT (o herramientas de acceso remoto), troyanos bancarios, *infostealers,* entre otras amenazas. Además, casi todos los códigos maliciosos contienen algún tipo de módulo o funcionalidad que involucra acciones asociadas a los anteriores.[2]

CUARTO. – El incremento del cibercrimen como negocio provoca año a año un aumento de demanda y dinero circulante en los mercados clandestinos. Esto trajo consigo una nueva tendencia, a partir del año 2021: la exposición de los mercados oscuros en sitios y redes de acceso sencillo. En otras palabras, los cibercriminales ya no deben acceder a lugares ocultos de la internet para poder obtener métodos de ataque, amenazas o información de sus víctimas, sino que estos se encuentran a algunos clics de distancia, disponibles para quien lo solicite tanto en sitios de la web superficial como en redes sociales anónimas como *Telegram*. Con la facilidad de acceder a los recursos necesarios para cometer un ataque informático, combinado con los millones de dólares que el cibercrimen mueve, es lógico ver por qué cada vez más personas se unen al mundo del

[2] Ver: https://eset-la.com/Public_files/ESET-security-report-LATAM2022.pdf?utm_campaign=latam-es-online-esr_%2B5&utm_medium=email&utm_source=Eloqua&elqTrackId=fbf5868105714f7d9aa7acbe6723519a&elq=4563b4da88b6410db84959c71278649c&elqaid=2834&elqat=1&elqCampaignId, 7 de octubre de 2022.

cibercrimen enfocado a corporaciones, lo cual resulta en un incremento sostenido de ataques.[3]

QUINTO. - El ***ransomware*** continúa siendo una amenaza que figura constantemente en titulares de ciberamenazas y ataques, particularmente aquellos orientados a compañías. Sin ir más lejos, y según datos revelados por la oficina de Control de Crímenes Financieros (FinCEN) de los Estados Unidos, solo en este país entre enero y junio de este año el promedio mensual de transacciones en Bitcoin que se sospecha están relacionadas con el ***ransomware*** es de 66.4 millones de dólares. Solo en el ataque a Kaseya, compañía prestadora de servicios que fue víctima intermedia de un ataque a la cadena de suministros, los operadores detrás del ***ransomware*** REvil demandaron un pago de 70 millones de dólares por la herramienta de descifrado para que las víctimas pudieran recuperar los archivos secuestrados.[4]

V. PERSPECTIVA DE GÉNERO.

De conformidad con la *Guía para la Incorporación de la perspectiva de género en el trabajo legislativo del Congreso de la Ciudad de México*[5], donde se señala que "la perspectiva de género tiene entre sus objetivos, erradicar las diversas causas que llevan a las circunstancias opresoras en las que desde siempre hemos tenido que desarrollarnos las mujeres por la simple razón de serlo, y con esta afirmación, no intento menospreciar el género, pero sí anteponer nuestra condición de personas sujetas de derechos, sin que

[3] Ver: https://eset-la.com/Public_files/ESET-security-report-LATAM2022.pdf?utm_campaign=latam-es-online-esr_%2B5&utm_medium=email&utm_source=Eloqua&elqTrackId=fbf5868105714f7d9aa7acbe6723519a&elq=4563b4da88b6410db84959c71278649c&elqaid=2834&elqat=1&elqCampaignId=, 8 de octubre de 2022.
[4] Ibídem.
[5] Ver: https://genero.congresocdmx.gob.mx/wp-content/uploads/2019/12/Gui%CC%81a-para-la-Incorporacio%CC%81n-de-la-perspectiva-de-ge%CC%81nero-en-el-trabajo-legislativo-del-Congreso-de-la-Ciudad-de-Me%CC%81xico-2.pdf, 3 de julio de 2022.

para el ejercicio de ellos medie alguna otra característica, lo cual resulta ser una aspiración que sigue sin cumplirse en ningún ámbito de la vida en sociedad."

En tal sentido, el presente instrumento legislativo utiliza un lenguaje incluyente y no sexista; que no discrimina, excluye, invisibiliza o estereotipa a las mujeres.

VI. RAZONAMIENTOS SOBRE SU CONSTITUCIONALIDAD Y CONVENCIONALIDAD.

A través del Convenio de Budapest sobre el Delito Cibernético existe una directriz internacional, también ampliamente utilizada en las Américas, que ayuda a los países a cumplir estos requerimientos. En referencia a la ley sustantiva, requiere que las partes penalicen el acceso ilícito, la interceptación ilegal, la interferencia de datos, la interferencia de sistemas, el uso indebido de aparatos, la falsificación informática, el fraude informático, la pornografía infantil y delitos relativos a las infracciones en materia de derechos de autor y derechos relacionados.

VII. ORDENAMIENTOS A MODIFICAR.

Se adiciona un Artículo 211. bis. 5.1. al Código Penal Federal.

VIII. CUADRO COMPARATIVO.

TEXTO VIGENTE CÓDIGO PENAL FEDERAL	**PROPUESTA NORMATIVA** CÓDIGO PENAL FEDERAL
Sin correlativo.	**Artículo 211. bis. 5. 1.** Al que sin derecho y sin consentimiento de quien legalmente deba otorgarlo se apodere,

	altere, utilice, trafique, transgreda o transmita, datos reservados de carácter privado de una persona, que se hallan almacenado de manera telemática o en cualquier otro archivo de registro digital público o privado, con la finalidad de obtener para si o para otra persona un lucro indebido, o menoscabar la honra, la dignidad o el honor, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

IX. TEXTO NORMATIVO PROPUESTO.

ÚNICO. - Se adiciona un Artículo 211. bis. 5.1. al Código Penal Federal, para quedar como sigue:

Artículo 211. bis. 5. 1. Al que sin derecho y sin consentimiento de quien legalmente deba otorgarlo se apodere, altere, utilice, trafique, transgreda o transmita, datos reservados de carácter privado de una persona, que se hallan almacenado de manera telemática o en cualquier otro archivo de registro digital público o privado, con la finalidad de obtener para si o para otra persona un lucro indebido, o menoscabar la honra, la dignidad o el honor, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

X. ARTÍCULOS TRANSITORIOS.

ÚNICO. - El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

XI. LUGAR, FECHA, NOMBRE Y RÚBRICA DE QUIENES LA PROPONGAN.

En la Ciudad de México, dado en el Palacio Legislativo del Congreso de la Ciudad de México, a los 11 días del mes de octubre de 2022.

A T E N T A M E N T E.

Alberto Martínez Urincho

ALBERTO MARTÍNEZ URINCHO.
DIPUTADO.