

Año: 2020

Expediente: 13333/LXXV

H. Congreso del Estado de Nuevo León



LXXV Legislatura

PROMOVENTE: DIP. ITZEL SOLEDAD CASTILLO ALMANZA, E INTEGRANTES DEL PARTIDO ACCION NACIONAL

ASUNTO RELACIONADO: PRESENTA INICIATIVA DE REFORMA DEL CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEON, EN RELACION A DELITOS CIBERNETICOS.

INICIADO EN SESIÓN: 17 de febrero del 2020

SE TURNÓ A LA (S) COMISION (ES): Justicia y Seguridad Pública

C.P. Pablo Rodríguez Chavarría

Oficial Mayor



DIP. JUAN CARLOS RUÍZ GARCÍA
PRESIDENTE DEL H. CONGRESO DEL ESTADO DE NUEVO LEÓN
PRESENTE.-

Los suscritos, ciudadanos **Diputada Itzel Soledad Castillo Almanza** e integrantes del Grupo Legislativo del Partido Acción Nacional de la LXXV Legislatura del H. Congreso del Estado de Nuevo León, con fundamento en lo dispuesto en los artículos 68 y 69 de la Constitución política del Estado de Nuevo León, y con fundamento en el artículo 123 del Reglamento para el Gobierno Interior del Congreso del Estado de Nuevo León, me permito proponer el siguiente proyecto de Iniciativa de **reforma del Código Penal para el Estado de Nuevo León**, al tenor de la siguiente:

EXPOSICIÓN DE MOTIVOS

En 1995, en pleno nacimiento de Internet tal y como hoy lo conocemos, el Manual de Prevención y Control de los Crímenes Informativos de las Naciones Unidas, reflejó que el delito cibernético abarcaba mucho más que los actos criminales dirigidos contra datos o las infracciones de contenidos de derechos de autor, extendiéndolo a actividades tan diversas como el fraude, la falsificación, la pornografía infantil, el acceso no autorizado, el acoso, etc.



Symantec, una de las compañías más prestigiosas desarrolladora de software antivirus y especialidad en seguridad informática, define el delito informático como cualquier delito cometido en el que haya utilizado un equipo, una red o un dispositivo de hardware. Por tanto, podemos deducir que todo acto delictivo también será delito cibernético cuando se haga uso de hardware y o internet, de tal manera que la variedad de delitos cibernéticos es inmensa.

Durante la celebración del Congreso sobre Prevención del Delito y Justicia Penal, de la Organización de las Naciones Unidas en 2015, se habló del delito cibernético como una forma emergente de la delincuencia transnacional y uno de los de más rápido crecimiento “a medida que Internet se ha convertido en una parte casi esencial de nuestras vidas, suministrando información y comunicación en todo el mundo, los delincuentes le han sacado provecho. Con unos dos mil millones de usuarios en todo el mundo, el ciberespacio es el lugar ideal para los delincuentes, ya que pueden permanecer en el anonimato y tener acceso a todo tipo de información personal que, a sabiendas o inconscientemente, guardamos en línea. Las amenazas a la seguridad en Internet se han disparado en forma espectacular en los últimos años y el delito cibernético afecta ahora a más de 431 millones de víctimas adultas a nivel mundial



De acuerdo a la Encuesta Nacional sobre Disponibilidad y uso de TIC en hogares (ENDUTIH), en 2018 el número de mexicanos con acceso a internet eran 74 millones, la encuesta reveló que el 93% se conectan a internet desde el teléfono celular, 33% desde laptop, 32% en computadoras de escritorio.

La ONU en su Congreso sobre prevención del Delito y Justicia Penal menciona que el delito cibernético ha ido creciendo más fácilmente a medida que avanza la tecnología y los autores ya no requieren grandes habilidades o técnicas para ser una amenaza. Por ejemplo, las herramientas de software que permiten al usuario localizar puertos abiertos o anular la protección de contraseña se pueden comprar fácilmente en línea. Lo que no ha crecido fácilmente, por desgracia, es la capacidad para encontrar a los responsables. Con el anonimato que ofrece el ciberespacio, es difícil para las fuerzas del orden identificar y localizar a los delincuentes. Lo que se sabe, sin embargo, es que más de tres cuartas partes de la delincuencia cibernética están hoy vinculadas a la actividad de la delincuencia organizada.

La delincuencia cibernética ha crecido rápidamente, sin una normativa adecuada y una capacidad insuficiente en muchos países, la lucha contra la delincuencia cibernética es difícil. Se necesita un esfuerzo mundial para proporcionar una mejor protección y regulaciones más firmes porque los delincuentes cibernéticos hasta ahora se han escondido dentro de vacíos legales en los países con menos



reglamentación. Los autores y sus víctimas pueden ser localizados en cualquier lugar, pero los efectos se ven a través de las sociedades, destacando la necesidad de una respuesta internacional urgente y enérgica.

Según el “Convenio de Ciberdelincuencia del Consejo de Europa”, ratificado en el año 2001, los delitos informáticos o delitos cibernéticos pueden subdividirse en cuatro grupos:

1. *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:*

- *Acceso ilícito a sistemas informáticos.*
- *Interceptación ilícita de datos informáticos.*
- *Interferencia en el funcionamiento de un sistema informático.*
- *Abuso de dispositivos que faciliten la comisión de delitos.*

2. *Delitos informáticos:*

- *Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.*
- *Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.*

3. *Delitos relacionados con el contenido:*



- *Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.*

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines, como la copia y distribución de programas informáticos, o la piratería informática.

Otra clasificación hace referencia a la frecuencia del delito respecto de la persona perjudicada. En este sentido, podemos agrupar los delitos cibernéticos en dos grupos:

Delitos cibernéticos de tipo I, aquellos que, desde la perspectiva de la víctima, se producen en una única ocasión, por ejemplo el phishing, o la instalación de un malware en un ordenador para espiar a la víctima. Son delitos en los que también suele ser habitual, aunque no imprescindible, el uso de algún tipo de programa malicioso para registrar la actividad de la víctima aprovechando los fallos de seguridad del navegador, del propio sistema operativo... También la usurpación de identidad, el fraude, la piratería, etcétera. forman parte de los delitos cibernéticos de tipo I.

Delitos cibernéticos de tipo II son los que se suceden de forma repetida, incluso persistente. En estos casos el ciberdelincuente interactúa con la víctima en varias ocasiones. Hablamos del chantaje, la extorsión, el



acoso, el espionaje industrial, la planificación de actividades terroristas, etcétera.

Debido a la complejidad que presenta el tema, cuando se comete un delito cibernético, el juez no entiende cómo se lleva a cabo la conducta y le es muy difícil encuadrar el delito informático en un tipo penal existente. En derecho penal es requisito que la ley específica describa la conducta, luego tienes que comprobar que cada punto se cumplió. “Entonces, si la conducta no está descrita como tal, a detalle y con la redacción que está prevista en el Código, no puedes hacer nada. Si te falta un elemento, no hay delito que perseguir y dejan libres a los ciberatacantes”. Es por lo anterior necesario establecer en nuestro Código Penal un Capítulo relativo a los “Delitos Cibernéticos” en donde se estipulen adecuadamente los elementos del delito como lo son: conducta, tipicidad, antijuricidad, culpabilidad, imputabilidad, punibilidad y condicionalidad objetiva.

Por lo anteriormente expuesto que acudimos a promover el siguiente Proyecto de Reforma

DECRETO

UNICO. - Se reforma el párrafo tercero del artículo 385; la fracción V al artículo 223 Bis; y se adiciona un párrafo segundo al artículo



161 Bis 2, un párrafo segundo al artículo 236, un quinto párrafo al artículo 292, un párrafo segundo al artículo 343, un párrafo segundo al artículo 345, 345, y los artículos 439 Bis, 429 Bis 1 y 429 Bis 2, todos del Código Penal para el Estado de Nuevo León para quedar como sigue:

Artículo 161 Bis 2.- (...)

Al que, con intención de atentar contra la paz o seguridad pública, utilice medios de comunicación como teléfono, radio, Internet o cualquier otro medio electrónico con el fin de dar aviso de una falsa emergencia que provoque la movilización o presencia de personal de emergencia, como ambulancias, protección civil, bomberos o elementos de corporaciones de seguridad pública o de procuración de justicia se le aumentará la pena hasta en una mitad

Artículo 223 Bis.- (...)

- I. (...)**
- II. (...)**
- III. (...)**
- IV. (...)**
- V. Al que sin autorización modifique, elimine o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a él.**



Artículo 236.- (...)

La sanción se agravará hasta en una mitad a quien lo realice utilizando cualquier medio de comunicación como teléfono, radio, Internet o cualquier otro medio electrónico.

Artículo 292.- (...)

La sanción se agravará hasta en una mitad a quien la realice utilizando cualquier medio de comunicación como teléfono, radio, celular, Internet o cualquier otro medio electrónico.

Artículo 343.- (...)

Se aumentará la pena hasta en una mitad cuando se utilicen medios de comunicación como teléfono, radio, Internet o cualquier otro medio electrónico.

Artículo 345.- (...)

Se aumentará la pena hasta en una mitad cuando se utilicen medios de comunicación como teléfono, radio, Internet o cualquier otro medio electrónico.



385.- (...)

(...)

I. ...

II. ...

III. ...

Además de la pena que le corresponda conforme a las fracciones anteriores, se impondrá de dos a ocho años de prisión cuando se haya utilizado la publicidad por cualquier medio de comunicación masivo, **cuando se utilice cualquier medio de comunicación electrónico o bien cuando se encuadre en la hipótesis establecida en la fracción XIV del artículo 386.**

429 BIS.- Al que estando autorizado para acceder a sistemas o equipos de informática de alguna entidad pública, indebidamente en perjuicio de otro o del servicio público modifique, elimine o provoque pérdida de información, se le impondrán de tres a ocho años de prisión y multa de doscientas a seiscientas cuotas.

429 Bis 1.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna entidad pública indebidamente copie, transmita o imprima información ocasionando un daño, se



le impondrán de uno a cuatro años de prisión y multa cien a trescientos cuotas.

429 Bis 2.- Al que valiéndose de equipos informáticos o de información utilice indebidamente datos o información personal de otro para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero, se le impondrán de seis meses a dos años de prisión y multa de cien a trescientas cuotas.

TRANSITORIO

UNICO.- El presente Decreto entrará en vigor el día siguiente al de su publicación en el Periódico Oficial del Estado.

ATENTAMENTE

Monterrey, Nuevo León a 17 de febrero 2020

Dip. Carlos Alberto de la Fuente Flores

Dip. Itzel Soledad Castillo Almanza

Dip. Claudia Gabriela Caballero Chávez



H. CONGRESO DEL ESTADO DE NUEVO LEÓN
LXXV Legislatura
GRUPO LEGISLATIVO DEL PARTIDO ACCIÓN NACIONAL

Dip. Eduardo Leal Buenfil

Dip. Félix Rocha Esquivel

Dip. Jesús Ángel Nava Rivera

Dip. Juan Carlos Ruiz García

Dip. Leticia Marlene Benvenutti Villarreal

Dip. Lidia Margarita Estrada Flores

Dip. Luis Alberto Susarrey Flores

Dip. Mercedes Catalina García Mancillas

Dip. Myrna Isela Grimaldo Iracheta

Dip. Nancy Aracely Olguín Díaz



H. CONGRESO DEL ESTADO DE NUEVO LEÓN
LXXV Legislatura
GRUPO LEGISLATIVO DEL PARTIDO ACCIÓN NACIONAL

Dip. Rosa Isela Castro Flores

Dip. Samuel Villa Velázquez