LEGISLAR & CASTIGAR

EL PUNITIVISMO PENAL EN NOMBRE DE LA CIBERSEGURIDAD

R3D
Red en Defensa
de los Derechos Digitales

Leslie Jiménez Urzua
Grecia Macías Llanas
Francia Pietrasanta Baldazo

R3D
Red en Defensa
de los Derechos Digitales

GLOBAL
PARTNERS
DIGITAL

ÍNDICE

I. INTRODUCCIÓN 01

A. ¿QUÉ ES LA CIBERSEGURIDAD? 03

II. CIBERSEGURIDAD CON PERSPECTIVA DE DERECHOS HUMANOS. 03

B. ESTÁNDARES BÁSICOS DE DDHH Y CIBERSEGURIDAD. 05

¿Qué derechos humanos se pueden ver afectados en el contexto de ciberseguridad? 06

C. LA SECURITIZACIÓN DE LA CIBERSEGURIDAD Y EL ALZA DE PUNITIVISMO EN LEYES DE DELITOS INFORMÁTICOS. 08

Diferencia entre ciberseguridad y delitos informáticos. 08

El punitivismo en la legislación de ciberseguridad 09

La influencia de Budapest y la ciberseguridad en entornos internacionales 12

Criterios internacionales sobre disposiciones penales respecto a ciberseguridad 17

D. DIAGNÓSTICO GENERAL 22

Derecho Penal y Teoría del Delito 22

Resumen general del análisis 24

Resumen específico de las iniciativas 25

1) Iniciativas de la Senadora Jesús Lucía Trasviña Waldenrat (MORENA) 25

2) Iniciativa del Senador Miguel Ángel Mancera Espinosa (PRD) 31

3) Iniciativa del Senador Gustavo Madero Múñoz (PAN) 34

E. RECOMENDACIONES GENERALES 37

III. ANEXOS 42

I. ELEMENTOS DEL DELITO 42

II. ANÁLISIS DE LA INICIATIVA DE LA SENADORA LUCÍA TRASVIÑA 44

Conceptos y tipos penales descritos en la iniciativa de la Senadora Lucía Trasviña 43

Delitos contra la confidencialidad, la Integridad y la disponibilidad de la Información 52

Elemento normativo 52

Elemento objetivos o descriptivos 52
Elementos subjetivo 53

Delitos contra el patrimonio 54

Elemento normativo 54
Elementos objetivos o descriptivos 54
Elementos subjetivo 54

Delitos contra la libertad de las personas 55

Elemento normativo 55
Elemento objetivos o descriptivos 55
Elementos subjetivo 56

Delitos sexuales 58

Elemento normativo 58
Elemento objetivos o descriptivos 58
Elementos subjetivo 59

Delitos contra la propiedad intelectual. 60

Elemento normativo 60
Elemento objetivos o descriptivos 60
Elementos subjetivo 61

Delitos contra la nación. 62

Elemento normativo 62

Elementos objetivos o descriptivos 62

Elementos subjetivo 63

Delitos contra el sistema financiero 64

Elemento normativo 64

Elementos objetivos o descriptivos 64

Elementos subjetivo 65

II. ANÁLISIS DE LA INICIATIVA DEL SENADOR MIGUEL ÁNGEL MANCERA. 66

Conceptos y tipos penales descritos en la iniciativa del Senador Miguel Ángel Mancera. 66

Delitos contra la Infraestructura de Informática Crítica 70

Elemento normativo 70

Elementos objetivos o descriptivos 70

Elementos subjetivo 71

Delitos en contra de los Sistemas Informáticos 72

Elemento normativo 72

Elemento objetivos o descriptivos 72
Elementos subjetivo 73

Delitos contra las personas usuarias. 74

Elemento normativo 74
Elemento objetivos o descriptivos 74
Elementos subjetivo 75

Delitos contra la ciberseguridad. 76

Elemento normativo 76
Elemento objetivos o descriptivos 76
Elementos subjetivo 77

II. ANÁLISIS DE LA INICIATIVA DEL SENADOR GUSTAVO MADERO MÚÑOZ 78

Conceptos y tipos penales descritos en la iniciativa del Senador Madero. 78

Delitos contra las redes de telecomunicaciones. 80

Elemento normativo 80
Elemento objetivos o descriptivos 80
Elementos subjetivo 81

Delitos contra las personas usuarias 82

Elemento normativo 82

Elemento objetivos o descriptivos 82

Elementos subjetivo 83

Delitos contra el Estado. 84

Elemento normativo 84

Elemento objetivos o descriptivos 84

Elementos subjetivo 85

Delitos contra el sistema financiero 86

Elemento normativo 86

Elemento objetivos o descriptivos 86

Elementos subjetivo 87

I. INTRODUCCIÓN

La tendencia legislativa en México ha demostrado que existe una seria confusión conceptual con respecto a la ciberseguridad y los delitos informáticos. La securitización de la ciberseguridad y el auge del punitivismo en el país ha desarrollado en las personas legisladoras la falsa creencia de que la ciberseguridad se aborda únicamente a través de la creación de delitos informáticos.

Esta perspectiva deja de lado toda la perspectiva integral de la seguridad informática y la protección de los derechos humanos en el entorno digital. En especial, olvida que la seguridad informática se encarga primordialmente de proteger a las personas y la información que es almacenada en la infraestructura digital.

En este informe, buscamos desmitificar los conceptos alrededor de la ciberseguridad y los delitos informáticos. Además, analizamos algunas de las iniciativas de ciberseguridad que han sido recientemente presentadas. Estas iniciativas reflejan la tendencia legislativa en México, la cual hasta el momento se ha limitado a proponer nuevos tipos penales para abordar el tema de ciberseguridad.

Existe una serie de patrones comunes en la forma de crear nuevos tipos penales sobre delitos informáticos en nuestro país. Las principales observaciones que encontramos son las siguientes:

I. El abuso del prefijo "ciber" que complejiza y obstaculiza la aplicación de la ley penal.

II. Términos vagos y amplios que sobre criminalizan conductas legítimas, en especial relacionadas con investigadores de seguridad.

III. La ausencia de los elementos del tipo penal relacionados con la intencionalidad y el daño provocado. Esta redacción resulta en la criminalización de personas por ejercer su labor como investigadores de seguridad y personas que modificaron un archivo por error.

IV. La criminalización de conductas legítimas protegidas por los derechos humanos como la libertad de expresión, el acceso a la cultura y acceso a la información.

II. CIBERSEGURIDAD CON PERSPECTIVA DE DERECHOS HUMANOS

A. ¿QUÉ ES LA CIBERSEGURIDAD?

Cuando hablamos de ciberseguridad o seguridad informática, muchas personas pensamos en mundos digitales, *hackers* o infraestructura tecnológica compleja. Hay muchas variaciones en la definición de ciberseguridad. El Grupo de Trabajo 1 de la Freedom Online Coalition definió recientemente la ciberseguridad como:

"La ciberseguridad es la preservación - a través de políticas públicas, tecnología y educación- de la accesibilidad, confidencialidad e integridad de la información y su infraestructura subyacente con el fin de mejorar la seguridad de las personas en línea y fuera de línea"[1].

Esta definición reconoce los elementos esenciales de la ciberseguridad pero pone la seguridad de las personas en el centro. En muchos espacios, la discusión de ciberseguridad se concentra en aspectos de seguridad nacional y la protección de la información de empresas privadas. Por eso, es complicado encontrar una definición que hable de la perspectiva de derechos humanos y social de la ciberseguridad.

---

1. Freedom Online Coalition. Why Do We Need a New Definition for Cybersecurity? Consulta en: https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity/?hilite=cybersecurity

Hay que desglosar la definición para ayudar a ilustrar los aspectos más importantes de la ciberseguridad. En primer lugar, la ciberseguridad no solo implica la generación de tecnología de seguridad, sino también las políticas públicas y educación son partes esenciales para el ecosistema de seguridad.

Existe un enfoque desproporcionado en buscar mejorar la ciberseguridad con tecnología compleja y costosa. No obstante, la mayor parte de las vulneraciones en la seguridad informática en organizaciones se debe a un error humano[2]. Esto no implica que la responsabilidad sea individualizada, más bien habla de una falta de prácticas institucionales para evitar riesgos y mitigar daños. Muchos actores del ecosistema digital no tienen políticas mínimas de seguridad y esto ha tenido efectos graves en infraestructuras críticas para la población.

La confidencialidad, integridad y accesibilidad de la información[3], también conocida como la tríada CIA, son componentes que se encuentran en varias definiciones.

» La accesibilidad se refiere a que la información debe estar disponible para las personas que lo necesitan. Este objetivo incluye que los servicios de infraestructuras digitales sean estables, que puedan ser accesibles de manera equitativa para todas las personas.

» La confidencialidad implica que la información debe de ser privada y evitar accesos no autorizados por los titulares de la información.

» El principio de integridad establece que la información almacenada debe de ser precisa, confiable, que no haya sido alterada sin consentimiento o tenga archivos dañados.

---

2. Ver. World economic Forum. The Global Risks Report 2022. Consulta en: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

3. Sharp Robin. Introduction to Cybersecurity: A multidisciplinary challenge. Springer 2023.

Finalmente, esta definición de ciberseguridad incluye como objeto de protección la infraestructura subyacente de la información. Es importante esta mención porque enfatiza el rol que tiene la infraestructura crítica en la vida de las personas y que su mantenimiento también es vital para que las personas puedan acceder a servicios esenciales.

B. ESTÁNDARES BÁSICOS DE DDHH Y CIBERSEGURIDAD

Desde el 2013, Naciones Unidas ha reconocido que los mismos derechos aplicables al entorno offline son aplicables en línea. Esto fue un parteaguas para poder establecer medidas para efectivamente proteger derechos humanos en entornos digitales. Dicho reconocimiento implica que la ciberseguridad también tiene una perspectiva de derechos humanos a considerar si se busca proteger efectivamente a las personas en un espacio digital.

La FOC igualmente hizo recomendaciones sobre cómo asegurar un piso mínimo para que las leyes y políticas públicas alrededor de la ciberseguridad sean consistentes con los derechos humanos.

Dentro de esas recomendaciones, incluyen que la perspectiva de derechos humanos sea considerada siempre antes de iniciar el desarrollo de leyes o políticas públicas sobre seguridad. Igualmente, que esta perspectiva considere a las personas que están en un especial grado de vulnerabilidad y son desproporcionadamente impactadas por las políticas de ciberseguridad.

¿QUÉ DERECHOS HUMANOS SE PUEDEN VER AFECTADOS EN EL CONTEXTO DE CIBERSEGURIDAD?

La ciberseguridad está relacionada con distintos derechos como por ejemplo, el derecho a la privacidad, libertad de expresión y acceso a las tecnologías de información y comunicación.

Distintas organizaciones de la sociedad civil han documentado ejemplos de cómo legislaciones y políticas públicas relacionadas con la ciberseguridad han sido usadas como pretexto para violar derechos humanos. A continuación, iremos desagregando los principales derechos afectados en el contexto de ciberseguridad.

Privacidad. El objetivo de proteger la seguridad de la información implica buscar que la información personal de personas como registros médicos, actividad comercial o datos bancarios se mantenga de manera privada y confidencial.

Estos datos sensibles que son almacenados por entes privados o gubernamentales y mantienen perfil pueden revelar fácilmente información sensible de las personas como sus afiliaciones políticas, religión, identidad de género, orientación sexual, y sensibles sobre una persona, entre otros[4].

Legislaciones o política pública sobre ciberseguridad han establecido erróneamente medidas que en vez de proteger a las personas terminan en vulneración de su seguridad. Por ejemplo, propuestas que vulneran el cifrado y la tecnología que protege la inviolabilidad de las comunicaciones.

Libertad de expresión. En entornos digitales, el derecho a la privacidad está estrechamente relacionado con el derecho a la libertad de expresión.

4. Fundación Karisma. "Guía de Viaje al Mundo Digital. Políticas de ciberseguridad para las personas defensoras de derechos humanos. 2020. Consulta en: https://archive.org/details/guia-ciberseguridad-l.-a

Existen casos donde propuestas legislativas de seguridad han establecido medidas de vigilancia en entornos digitales sin controles democráticos.

Este tipo de medidas tiene un impacto directo en la libertad de expresión. La vigilancia genera un efecto inhibitorio en personas que dependen de su privacidad para poder expresar sus ideas de manera libre.

De igual forma, bajo la perspectiva punitivista de ampliar el catálogo de delitos penales, se ha propuesto sancionar conductas relacionadas con la libre expresión de ideas en el entorno digital.

Esto incluye criminalizar conductas como "el esparcimiento de información falsa", la crítica a autoridades estatales, la incitación al ataque de "instituciones democráticas", etcétera. Este tipo de delitos busca poder controlar los discursos críticos y afecta desproporcionadamente a grupos vulnerables como investigadores, periodistas y defensores de derechos humanos.

Acceso y uso de las TIC. Este derecho a su vez habilita el ejercicio de otros derechos en el entorno digital, como el derecho a la educación y el acceso a la información.

El enfoque punitivo de las políticas de ciberseguridad suele pasar por alto los principales obstáculos para el ejercicio de este derecho, como la brecha digital y la exclusión de los grupos en situación de vulnerabilidad (personas no heteronormadas, mujeres, personas de la comunidad LGBTIQ+, infancias, entre otros).

Algunas iniciativas legislativas proponen medidas que vulneran el acceso y uso de las TIC al permitir el monitoreo de redes y tráfico de Internet por parte de actores gubernamentales y privados, la exigencia de colaboración de plataformas y proveedores de Internet sin ningún control y la imposición de entregar "información de identidad real" para acceder a servicios de Internet. Estas propuestas reflejan cómo una política de ciberseguridad mal formulada puede tener efectos negativos en este derecho y en los derechos habilitados a través del acceso y uso de las TIC.

C. LA SECURITIZACIÓN DE LA CIBERSEGURIDAD Y EL ALZA DE PUNITIVISMO EN LEYES DE DELITOS INFORMÁTICOS

DIFERENCIA ENTRE CIBERSEGURIDAD Y DELITOS INFORMÁTICOS

La ciberseguridad es un área distinta al cibercrimen y la persecución de delitos informáticos. A pesar de que ambas materias hacen referencia a preservar la seguridad en espacios digitales, la ciberseguridad tiene una aproximación técnica en la preservación de la seguridad de sistemas computacionales, mientras que el cibercrimen se concentra solamente en el castigo de delitos informáticos ciberdependientes.

Una política de ciberseguridad puede establecer un marco de referencia que incluya distintas legislaciones y política pública. Esto incluye desde establecer políticas para manejar incidentes y crear equipos de respuesta hasta fortalecer en legislación la protección de datos personales[5].

Mientras tanto, el cibercrimen solamente se refiere a la persecución de delitos ciberdependientes. Estos delitos son aquellos que dependen irremediablemente de sistemas computarizados para poder realizarse, por ejemplo, el acceso ilegítimo con dolo a sistemas informáticos. Por otro lado, los delitos ciberhabilitantes son aquellos que pueden realizarse en el plano material y

---

5. Privacy International. "Understanding the difference between Cybersecurity and Cybercrime". 2018. https://privacyinternational.org/explainer-graphic/2273/understanding-difference-between-cyber-security-and-cyber-crime

digital, por ejemplo, el fraude. El fraude puede cometerse tanto en una página web falsa como en una llamada telefónica engañosa.

Los conceptos de ciberseguridad y cibercrimen son constantemente mezclados incorrectamente, incluso en espacios relevantes con tomadores de decisiones. Una de las razones de esta confusión es consecuencia de la securitización de la ciberseguridad y los entornos digitales.

La securitización de la ciberseguridad ha provocado que tomadores de decisiones establezcan medidas invasivas a los derechos humanos bajo la justificación de "proteger y mantener la seguridad del entorno digital y la seguridad nacional".

EL PUNITIVISMO EN LA LEGISLACIÓN DE CIBERSEGURIDAD

En los últimos años, la preocupación de los países por los riesgos de ciberseguridad se ha incrementado por el alza de delitos "ciberhabilitantes". Esto ha hecho que se haya visto la ciberseguridad y el combate al cibercrimen como solamente un asunto de seguridad pública y nacional.

La narrativa de que existen delincuentes o agentes malignos que pueden atacar en cualquier momento al país ha sido dominante en los principales espacios de toma de decisiones. Esto ha resultado en que erróneamente, tomadores de decisiones consideren que las restricciones a derechos humanos o criminalización de conductas legales son necesarias para "mantener la seguridad del ciberespacio".

La decisión de criminalizar conductas de manera selectiva ha sido una tendencia legislativa en México y Latinoamérica. Esta tendencia deriva de la falta de iniciativa para buscar respuestas de política pública que atiendan a las verdaderas causas detrás de estos fenómenos.

Cuando nos referimos al punitivismo, lo hacemos tanto a una característica de la política criminal[6] como a la opinión pública hacia el castigo de las personas infractoras y hacia el funcionamiento del sistema de justicia penal[7]. Esto porque el punitivismo al ser este discurso elaborado desde la estructura estatal, se dirige a justificar la intervención del derecho penal para solucionar cualquier problema social mediante la aplicación de un castigo irracional y desproporcionado, lo que reduce o elimina la posibilidad de evitar encontrarse dentro del sistema penal[8].

---

6. La política criminal es el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción. Véase, Tirado Misael y Cáceres, Tovar, "La política criminal frente al ciberdelito sexual contra niños, niñas y adolescentes en Colombia", Revista Científica General José María Córdova, Volumen 19, No. 36, octubre-diciembre 2021. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1900-65862021000401

7. Véase, Aguilar Jurado, Juan Antonio, "Aproximación al análisis de las actitudes punitivas", Revista Criminalidad, Volumen 60 , Número 1, Enero-abril 2018 , p. 99. Disponible en: http://www.scielo.org.co/pdf/crim/v60n1/1794-3108-crim-60-01-00095.pdf

8. El principio de *ultima ratio*, se refiere al principio de intervención mínima del derecho penal, que plantea que el derecho penal debe ser utilizado como último recurso, impone la necesidad de agotar medidas o mecanismos previos. Este principio obliga al poder legislativo al momento de crear normas penales considerar otras vías no criminalizadoras así como al poder judicial de replantear las sanciones consideradas en la norma penal para imponerlas. La asimilación de las normas, las disposiciones jurídicas y el funcionamiento del sistema de justicia penal deberían facilitar la construcción de puentes de confianza entre las personas y las instituciones desde el primer punto de contacto. Cfr, Moreno Hernández, Moisés, "Principios Rectores en el Derecho Penal", en *Liber ad honorem*: Sergio García Ramírez,UNAM-IIJ, t II, México, 1998, pp. 1309-1343. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/117/26.pdf

En ese sentido el punitivismo configura un sistema complejo que articula un lenguaje y dinámica propia que impide a grupos en situación de vulnerabilidad[9] experimentar un sentimiento de pertenencia o colectividad o una sensación de justicia y confianza, debido a que tiene como principal consecuencia criminalizarles.

Las principales características de una norma penal con perspectiva punitivista son[10]:

» **Volatilidad:** se refiere al comportamiento de la sociedad, el cual varía por diversos factores circunstanciales, como delitos de alto impacto social (delincuencia organizada, homicidio doloso, terrorismo, entre otros) o la adquisición de información relacionada con la delincuencia, la persona delincuente o con el funcionamiento del sistema penal.

» **Ambivalencia:** Se refiere a la forma en que reaccionan las personas ciudadanas ante la existencia de los delitos y sus sanciones. Es decir, un mismo ciudadano suele apoyar tanto medidas que implican castigo como otras encaminadas a la rehabilitación, la reinserción y la reparación, no decantándose de forma excluyente por una de estas opciones.

» **Heterogeneidad:** actitudes que no son uniformes, sino que varían en función de la gravedad del delito cometido.

---

9. En atención a la Agenda Regional de Desarrollo Social Inclusivo de la Comisión Económica para América Latina y del Caribe, se consideran grupos en situación de vulnerabilidad la niñez, adolescentes; personas jóvenes; personas mayores; mujeres; pueblos indígenas; población afrodescendiente; personas con discapacidad; personas que habitan en zonas rezagadas; personas lesbianas, gais, bisexuales, trans e intersexuales; las personas en situación de tránsito y aquellos desplazados por conflictos, y las poblaciones afectadas por los desastres y el cambio climático.

10. Aguilar Jurado, Juan Antonio, "Aproximación al análisis de las actitudes punitivas", op. cit.

El proceso de criminalización que realizan las normas penales con perspectiva punitivista se conduce a seleccionar a un reducido grupo de personas, a las que someten a su coacción con el fin de imponerles una sanción penal[11].

Los efectos de los procesos punitivistas es la instauración de subjetividades en la norma penal que dan lugar a la aparición del "del delincuente" que justifican una posición frente a la ley y la acción cometida, el rol del punitivismo es justificar el origen de la violencia estatal así como de las categorías otorgadas a las personas ubicadas como perpetradoras de un delito, por ejemplo, "violador" y "agresor" , desde una perspectiva que ignora problemáticas complejas que constituyen la acción delictiva y para lo que la explicación punitivista no ofrece respuestas ni soluciones[12].

LA INFLUENCIA DE BUDAPEST Y LA CIBERSEGURIDAD EN ENTORNOS INTERNACIONALES

a) Convenio sobre ciberdelincuencia

El Convenio Nº 185 del Consejo de Europa, sobre la ciberdelincuencia (Convenio de Budapest), firmado el 23 de noviembre de 2001 en Budapest Hungría, entrando en vigor el 1o de julio de 2004, es el primer tratado internacional multilateral vinculante que aborda los delitos informáticos para armonizar las leyes nacionales, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones.

---

11. Andrade, Eliana, et. al., Reportantes de vulnerabilidades en sistemas digitales ante la ley penal argentina, Democracia en la Red-O. D. I. A.-Fundación Vía Libre, p. 10. Disponible en: https://datosenfuga.org/static/media/DATOS%20EN%20FUGA_%20Reportantes%20de%20Vulnerabilidades.cc8440b556c836af3ef7.pdf

12. Véase, Yesuron Mariela Ruth, "Una lectura feminista y antipunitivista de la dicotomía víctima-victimario", Polémicas feministas, núm. 5, 2021. Disponible en: https://revistas.unc.edu.ar/index.php/polemicasfeminista/article/view/35690/35809

No obstante el convenio es producto de los trabajos del Consejo de Europa, actualmente de los 67 estados adheridos se encuentran también países no europeos[13], entre ellos Estados Unidos, Chile, Canadá, Argentina y Colombia, de igual manera se organizaciones como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT) se han adherido.

El convenio también identifica a estados observadores, los cuales pueden enviar observaciones para cooperar con el Consejo, siempre que estén dispuestos a aceptar los principios de la democracia, estado de derecho, respeto a los derechos humanos y libertades fundamentales. México es uno de esos países observadores[14].

Los 3 ejes primordiales de este instrumento son:

1. Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos;

2. Establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico, así como;

3. Establecer un régimen rápido y eficaz de cooperación internacional.

El documento se encuentra estructurado en cuatro capítulos: a) Terminología, b) Medidas que deberán adoptarse a nivel nacional – el derecho penal sustantivo y derecho procesal, c) Cooperación internacional y d) Cláusulas

13. Véase, países partes del Convenio de Ciberdelincuencia. Disponible en: https://www.coe.int/en/web/cybercrime/parties-observers

14. México de manera formal ha sido invitado a ascender y adherirse al Convenio, siendo la más reciente en septiembre de 2020.

finales. l Convenio de Budapest busca direccionar los procesos de tipificación de los estados a partir de descripciones que carecen de taxatividad penal, en atención a lo siguiente:

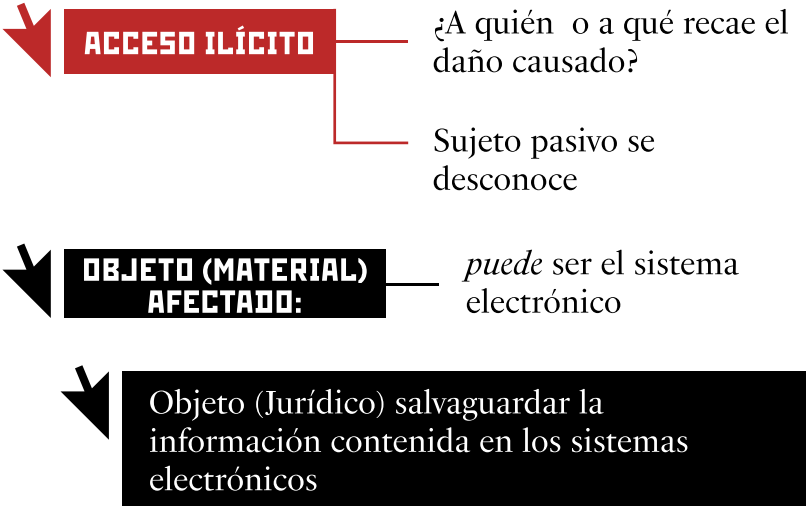
1. Noción legal

Las nociones legales contenidas en el Convenio de Budapest, fungen como directrices que de manera general describen conductas diversas con bienes jurídicos diversos.

2. Sujetos y objetos

No se identifica ni se asigna calidad de las personas intervinientes (sujetos del delito), eso resulta problemático pues crea incertidumbre jurídica en torno a cuáles serán los procesos de criminalización subjetivo que cada estado puede construir en torno a las nociones legales abiertas.

Respecto a los objetos, estos dependen en relación a las nociones legales, por ejemplo, en los dirigidos a aspectos patrimoniales la afectación recae en bienes muebles, como en el caso del fraude y los relacionados a la propiedad intelectual. Sin embargo, en el caso del acceso e interceptación ilícita, el objeto recae subjetivamente en la información personal del sujeto pasivo.

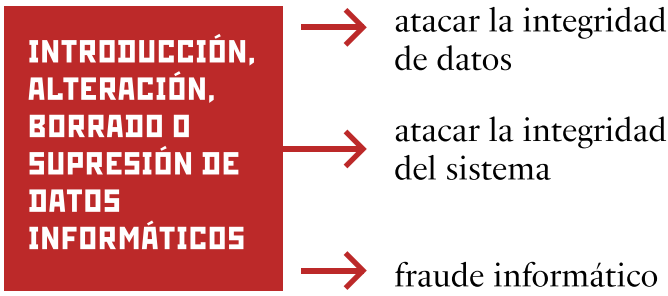


Los bienes jurídicos son un elemento esencial de los delitos, pues es derivado de ellos que el estado justifica la existencia y clasificación de los delitos, el Convenio es muy difuso al señalar qué bienes está proponiendo proteger.

3. Formas de manifestación del delito

Los delitos pueden darse de diversas maneras, surgiendo de igual manera varios resultados típicos. Es relevante tener en cuenta ello porque a partir de ello se resuelve cuándo un delito subsiste por sí mismo o se acumula con otra conducta, dando origen a un concurso de delitos.

Respecto a los delitos descritos en el Convenio, al parecer son conductas que pretenden subsistir sin la dependencia de la realización de otras conductas descritas. Sin embargo en el caso de los delitos de ataques a la integridad de datos y sistema las conductas enlistadas sí propician la existencia de un concurso de delitos.



b) Delitos cibernéticos internacionales

Dentro del análisis del derecho informático internacional, los delitos cibernéticos se asocian a conductas criminales de naturaleza patrimonial, las cuales son:

HACKING[15]	Tipificado como la conducta de acceder de manera no autorizada a un equipo o sistema informático.
CRACKING[16]	Tipificado como la conducta de atacar sistemas informáticos y software con intención maliciosa.
PHISHING[17]	Tipificado como la simulación de información, correspondiente a correo electrónico, red social, banco, institución pública, etc.) con el objetivo de robar información privada.
EVIL TWINS[18]	Tipificado como el engaño para obtener información mediante el uso de redes WiFi inalámbricas que aparentan ofrecer conexiones a internet confiables, como las que se encuentran en sitios públicos como restaurantes o lugares públicos.
PHARMING[19]	Tipificado como la vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (Domain Name) a otro ordenador diferente.
ROBO DE IDENTIDAD[20]	Es el robo de identidad, tanto de personas físicas y personas jurídicas.
CYBERTERRORISMO[21]	El ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno.

15. Piña Libien, Hiram Raúl, "Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano". Disponible en: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf

16. ídem.

17. Instituto Nacional de Ciberseguridad, Phishing, España. Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing

18. Piña Libien, Hiram Raúl, op. cit.

19. Rodríguez Magariños, Faustino Gudin, Nuevos delitos informáticos: Phishing, Pharming, Hacking y Cracking. Disponible en: https://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

CRITERIOS INTERNACIONALES SOBRE DISPOSICIONES PENALES RESPECTO A CIBERSEGURIDAD

En el ámbito del derecho internacional público el abordaje de la ciberseguridad ha sido principalmente desde la incorporación del prefijo ciber a conceptos como espacio, guerra, espionaje, terrorismo, delito, con un enfoque en la seguridad colectiva de los Estados.

Esto incluye trazar el espacio de aplicación de la norma internacional, describir la conducta a sancionar y las obligaciones de los estados, ¿Cuál es el límite o restricción de la jurisdicción de los estados y de la jurisdicción internacional?, ¿Cuál es el interés de la comunidad internacional frente a actividades concebidas en el espacio digital de las personas?. Las primeras labores jurídicas de esas interrogantes se desarrollaron desde el soft law de las Naciones Unidas.

c) Organización de las Naciones Unidas (ONU)

La aproximación realizada por ONU al tema de ciberseguridad, se ha dirigido hacia el mantenimiento de la paz y la seguridad internacionales desde la prevención del delito y justicia penal. Esto comenzó con la creación del Departamento de Asuntos de Desarme en 1998, el cual cambió su nombre a Oficina de Asuntos de Desarme de las Naciones Unidas[22] (UNODA, por sus

---

20. Piña Libien, Hiram Raúl, op. cit.

21. Corte Interamericana de Derechos Humanos, Biblioteca. Disponible en: https://www.corteidh.or.cr/sitios/tesauro/tr2652.htm

22. La UNODA es un organismo de la Secretaría General de la ONU que se encarga del desarme nuclear y la no proliferación. Además, fortalece los mecanismos para que se logre el objetivo principal de reducir las cantidades existentes de los diferentes tipos de armamento, que pueden ser, de destrucción masiva o convencional.

siglas en inglés) en el 2007 fue la que dio a la UNODA un enfoque hacia el aspecto de la seguridad de la información como asunto que puede afectar la estabilidad del sistema internacional, debido a su constante innovación en el marco de las TIC.

La resolución A/RES/53/70 "Los avances de la informatización y las telecomunicaciones en el contexto de la seguridad internacional" presentada por la Federación Rusa, la cual fue aprobada sin ser sometida a votación, expone los efectos que puede tener el uso indebido de las redes de telecomunicaciones y la informatización a la seguridad internacional, exhortando a los Estados para realizar estudios y diagnósticos sobre su situación en materia de seguridad cibernética.

Desde entonces, el Secretario General de la ONU ha presentado a la Asamblea General informes anuales que retoman las opiniones de los Estados miembros sobre seguridad de la información. El primer informe A/65/154, presentado el 20 de julio de 2010, recopila las observaciones y recomendaciones realizadas por Cuba, Grecia, México, Panamá, Qatar, Reino Unido de Gran Bretaña e Irlanda del Norte y Ucrania.

Lo referido por México en este informe puede dividirse en tres segmentos. El primero, plantea una evaluación general de los problemas de la seguridad de la información, en el que reconoce que no existe una política de seguridad cibernética que guíe las estrategias del combate al cibercrimen en el país, porque lo que sugiere que la legislación en la materia sea fortalecida, para que los jueces cuenten con instrumentos que les permitan atender y sancionar los ciberdelitos.

El segundo punto se refiere a las medidas que se adoptan a nivel nacional para fortalecer la seguridad en la información y contribuir a la colaboración internacional, en este punto manifestó la necesidad de regular delitos que

permitan otorgar seguridad a la información. Finalmente en el tercer rubro sugiere acciones que la comunidad internacional podría implementar para robustecer los esquemas en ese plano a escala mundial.

Otro órgano de la ONU que ha debatido sobre la ciberseguridad es la Asamblea General (AGNU). Desde su Primera Comisión[23] y Tercera Comisión[24] estableció dos grupos estratégicos de trabajo sobre ciberseguridad: el Comité intergubernamental especial de expertos de composición abierta (OECE por sus siglas en inglés de Open-ended ad hoc intergovernmental committee of experts)[25] y el Grupo de Expertos Gubernamentales (GEG).

Derivado del primer estudio del GEG, en el año 2011 la Asamblea General aprobó la resolución A/RES/66/24, que solicitó un grupo de expertos para determinar los riesgos y amenazas al orden público de los Estados. Además, en el informe bienal 2013-2014 del GEG A/68/98, se estableció que el marco jurídico de la seguridad de la información corresponde al derecho internacional público, pues la problemática ocurre en el territorio de los Estados. Los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar.

En consecuencia y después de varios informes, en el año 2019 la Tercera Comisión de la AGNU comenzó la investigación del ciberdelito. Mediante la resolución A/C.3/74/L.11, creó el Comité intergubernamental especial de expertos de composición abierta (OECE) para comenzar a redactar una nueva convención de las Naciones Unidas sobre el ciberdelito.

---

23. La Primera Comisión se ocupa de los temas relativos a desarme y seguridad internacional. Véase: https://www.un.org/es/ga/first/index.shtml

24. La Tercera Comisión se ocupa de los asuntos sociales, humanitarios y culturales. Véase: https://www.un.org/es/ga/third/

25. Se encuentra integrado por todos los Estados miembros de las Naciones Unidas y se encarga de redactar una nueva Convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

En alcance a la resolución de la Tercera Comisión, el 20 de enero de 2020, la AGNU estableció en la resolución A/RES/74/247 un comité intergubernamental compuesto por expertos de todas las regiones para elaborar una convención internacional sobre la lucha contra el uso de las TIC con fines delictivos.

La necesidad de contar con una nueva convención también surge desde la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución. Ésta indicó la posibilidad de convocar un grupo de expertos para la realización de un estudio sobre problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado para la prevención, detección, investigación y el enjuiciamiento de esos delitos en todas sus formas con el fin de aumentar la seguridad de las redes informáticas de los Estados.

d) Sistema Interamericano

En el año 2003, la Organización de los Estados Americanos (OEA) aprobó la Resolución AG/RES.1939 (XXXIII-O/03), en la que encomendó desarrollar un proyecto que estudiara la ciberseguridad desde un enfoque multidimensional y multidisciplinario.

En el año 2004 se aprobó la Resolución AG/RES. 2004 (XXXIV-O/04), que lleva por título "Estrategia Interamericana Integral para combatir las Amenazas a la Seguridad Cibernética". Esta resolución confiere al

---

26. La SSM se encuentra integrada por cuatro dependencias que son: la Secretaría Ejecutiva de la Comisión Interamericana para el Control del Abuso de Drogas; la segunda es la Secretaría del Comité Interamericano Contra el Terrorismo; la tercera es el Departamento de Seguridad Púbica; y la cuarta es el Departamento contra la Delincuencia Organizada Transnacional. Véase: https://www.oas.org/es/ssm/template.asp?file=/es/ssm/about_spa.asp

CICTE las competencias para que integre la seguridad cibernética a sus funciones, por lo que crea la Secretaría de Seguridad Multidimensional[26] (SSM), la cual visualiza como riesgo de los Estados los ataques a la seguridad cibernética.

Los objetivos de la SSM en el ámbito cibernético son:

1. Establecer grupos nacionales de alerta, vigilancia y prevención, denominados Equipos de Respuesta a Incidentes (CSIRT, por sus siglas en inglés);

2. Crear una red de alerta hemisférica que proporcione formación técnica a personal que trabaje en la seguridad cibernética de los gobiernos;

3. Fomentar el desarrollo de Estrategias Nacionales sobre seguridad cibernética y;

4. Promover una cultura en seguridad cibernética que permita desarrollar conocimiento.

D. DIAGNÓSTICO GENERAL

DERECHO PENAL Y TEORÍA DEL DELITO

El objetivo del derecho penal[27] es establecer qué delitos, penas y medidas de seguridad son aplicables para el Estado con la finalidad de la permanencia del orden social[28]. Como se analizó en apartados anteriores, el derecho penal interviene para convertir hechos sociales a hechos punibles y atribuye responsabilidad jurídico-penal a determinado comportamiento antijurídico[29], lo cual provoca que el Estado reaccione con una sanción.

El concepto de delito se encuentra ubicado en el artículo 7 del Código Penal Federal, que refiere que el "delito es toda acción u omisión que sancionan las leyes penales"[30]. La dogmática penal de nuestro país se encuentra basada en la teoría quíntuple del delito, en la que se integra por los elementos de conducta, tipicidad, antijuricidad, culpabilidad y punibilidad. La descripción detallada de estos elementos se encuentran en el Anexo "Tabla elemen-

---

27. El Derecho Penal será entendido como un discurso normativo creado por el Estado, que establece conductas denominadas como delito, etiqueta personas como delincuentes y sanciona mediante la imposición de penas o medida de seguridad con lo que busca mantener el control social.

28. Véase, Calderón Martínez, Alfredo T, Teoría del Delito y juicio oral. Colección de Juicios Orales, UNAM-IIJ, 2da reimpresión, México, 2017, p. 2. Disponible en: https://biblio.juridicas.unam.mx/bjv/detalle-libro/3982-teoria-del-delito-y-juicio-oral-juicios-orales-numero-23, fecha de consulta: 14 de agosto de 2022.

29. Cfr., Kindhäuser Bonn, Urs, "La lógica de la construcción del delito", trad. Juan Pablo Mañalich R., Texto distribuido por Taller de Ciencias Penales de la UNMSM en el seminario realizado con la participación del Prof. Urs Kindhäuser del 23 al 25 septiembre 2009. Disponible en: https://www.pensamientopenal.com.ar/doctrina/35440-logica-construccion-del-delito

30. Artículo 7. Código Penal Federal. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

tos del delito".

Al crear una norma que busca tipificar (describir la conducta que será considerada antijurídica), las personas legisladoras deben respetar los principios constitucionales en materia penal que son:

a) Principio de mínima intervención

Se refiere a que el derecho penal únicamente *debe* proteger los bienes jurídicos más importantes frente a las formas más graves de agresión[31].

b) Principio de derecho penal de acto

La construcción de la norma penal no debe sancionar la personalidad de las personas sino el acto que se considere antijurídico[32].

c) Principio de taxatividad

Consiste en la prohibición de establecer tipos penales "abiertos", "vagos" e "imprecisos"[33], a fin de establecer certeza jurídica de las personas que habitan el Estado[34] y delimitar el alcance del poder punitivo[35]. Implica que los textos en los que se recogen los delitos describan claramente y con pre-

---

31. Artículo 17. Constitución Política de los Estados Unidos Mexicanos. Véase: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

32. Roxin, Claus: Derecho Penal: Parte General, Tomo I, Fundamentos: La estructura de la Teoría del Delito; Edit. Civitas, Madrid; 1997.

33. Véase, Suprema Corte de Justicia de la Nación, Acción de Inconstitucionalidad 149/2017. Comisión Nacional de los Derechos Humanos. 10 de octubre de 2019. Disponible: https://sjf.scjn.gob.mx/SJFSem/Paginas/DetalleGeneralScroll.aspx?ID=29663&Clase=DetalleSemanarioEjecutoriaBL#

34. Véase, Suprema Corte de Justicia de la Nación, Acción de Inconstitucionalidad 47/2016, Procuraduría General de la República. 11 de febrero de 2016. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5549996&fecha=11/02/2019#gsc.tab=0

35. Véase, Suprema Corte de Justicia de la Nación, Amparo en Revisión 1121/2016. Televisión Azteca, S.A., de C.V., 25 de octubre de 2017. Disponible en: https://sjf.scjn.gob.mx/SJFSem/Paginas/DetalleGeneralScroll.aspx?id=27513&Clase=DetalleTesisEjecutorias

cisión qué conductas están prohibidas, las sanciones penales que se pueden aplicar, quiénes la realizan y a quién o quiénes le recaen. Este principio se extiende hasta la imposibilidad de imponer penas por analogía o por mayoría de razón.

RESUMEN GENERAL DEL ANÁLISIS

El discurso punitivista ha provocado que la falta de criminalización de conductas en el "ciberespacio" sea apreciada como un falso vacío normativo, lo que ha alimentado la creencia errónea de que la ciberseguridad se logrará mediante el establecimiento de "ciberdelitos".

En los últimos años se ha intentado legislar en materia de ciberseguridad bajo la justificación que nuestro país requiere una "Estrategia Nacional de Ciberseguridad" y una ley que castigue los "ciberdelitos". En las LXIV y LXV legislaturas se han presentado diversas iniciativas que atienden a dicho enfoque.

Como analizaremos en los siguientes párrafos, estas propuestas contienen redacciones amplias sin salvaguardas y definiciones claras que generan incertidumbre sobre la protección efectiva a la libertad de expresión, acceso a la información y protección de datos de las personas. Además, algunas establecen la participación activa de las fuerzas armadas, lo cual puede dar lugar a actuaciones irregulares que violenten los derechos humanos.

En algunos casos, las iniciativas sugieren el establecimiento de delitos informáticos a partir de la incorporación de dichas conductas en el Código Penal Federal, como es el caso de la iniciativa del senador Gustavo Madero. Otras buscan proponer una ley de ciberseguridad para establecer delitos justificándose en la "seguridad nacional". Esto es problemático porque limita las iniciativas a la perspectiva del Estado y la protección de sus sistemas informáticos como fin último, lo cual deja de lado los derechos humanos de las personas.

A continuación, examinaremos tres de las iniciativas presentadas hasta el momento, a fin de ofrecer un análisis crítico sobre la tendencia de iniciativas de ley de ciberseguridad en México. Este análisis comprende comentarios sobre los conceptos, competencia, participación de fuerzas armadas, criminalización de conductas propuesta.

RESUMEN ESPECÍFICO DE LAS INICIATIVAS

1) Iniciativas de la Senadora Jesús Lucía Trasviña Waldenrat (MORENA)[36]

La senadora ha presentado tres iniciativas. Dos de ellas tendientes a crear una ley general de ciberseguridad o seguridad informática y una última que busca integrar el tema de ciberseguridad como de seguridad nacional.

Los textos presentados por la senadora resaltan los elementos típicos que justifican el proceso de criminalización legal tales como la selección de ciertas conductas que denotan vulnerabilidad, agregándoles peligrosidad y la percepción de amenaza.

» Conceptos

Las dos primeras iniciativas contienen un catálogo de palabras relacionadas con la terminología informática. Podemos dividir la estructura de este catálogo en dos categorías:

1. Las que sólo incorporan el prefijo ciber para "definir" conceptos de la ley.

---

36. Iniciativas de la senadora Senadora Jesús Lucía Trasviña Waldenrath http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/03/asun_3836691_20190327_1553013958.pdf http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/04/asun_4163509_20210406_1616512719.pdf

Estas definiciones contienen lenguaje centrado en la protección de la ciberseguridad del Estado y le asigna competencia exclusiva en esta área sin incluir la protección de las personas ciudadanas. Además, su amplitud e imprecisión generan confusión y falta de certeza, lo cual dificulta su aplicación efectiva.

2. Las que definen actividades digitales que justifican su criminalización legal.

Estos conceptos aumentan la problemática de las iniciativas, pues presentan definiciones inespecíficas y que replican o entremezclan conceptos con otros que también figuran en el catálogo. Además, incumplen con los requisitos de validez espacial de la ley penal que delimita el alcance de aplicación territorial de la norma penal al definir un "espacio de aplicabilidad intangible".

Los comentarios específicos de estas definiciones se encuentran en el "Anexo Análisis de la Iniciativa de la Senadora Lucía Trasviña".

» Competencia

Ambas iniciativas plantean una ley general. Es decir, que el funcionamiento de una política de ciberseguridad involucra la actividad de los tres niveles de gobierno (municipal, estatal y federal), los cuales deben salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones.

Sin embargo, indican que las entidades federativas se encargarán de conocer y resolver sobre los delitos cibernéticos del *fuero estatal* conforme a las legislaciones locales, lo cual obliga a que las propias entidades emitan la legislación respectiva para delimitar los delitos, por lo que no queda clara la delimitación de facultades de investigación y prevención delictiva. Además, la territorialidad se encuentra establecida de manera muy difusa, lo cual genera confusión en su aplicabilidad.

» Participación de las fuerzas armadas

La iniciativa presentada el 23 de marzo de 2021 identifica y reconoce la figura de la Guardia Nacional. Le asigna la capacidad de realizar de actos de investigación[37], tales como solicitar *sin intervención de la autoridad judicial* la cooperación de plataformas y empresas proveedoras de servicios de internet para neutralizar sitios, páginas electrónicas y perfiles de redes sociales. Esto aplica a delitos como terrorismo, la apología del odio nacional, racial, sexual o religioso, suplantación de identidad para fraude, y robo de datos personales, entre otros.

Igualmente, prevé la hipótesis de intervenir cuando se *dañe la imagen pública y la reputación de una persona o Institución*. Otra atribución que se le reconoce, es la preservación de la información, a los proveedores de servicios y contenidos en Internet, nacionales e internacionales cuando se pongan en riesgo las libertades, derechos humanos y otras garantías.

Esto es sumamente alarmante porque dota a la Guardia Nacional de la posibilidad de tener acercamiento con los proveedores para fiscalizar perfiles y publicaciones de usuarios, lo que pone en riesgo su información personal y su libertad de expresión.

Además, la última iniciativa propone el establecimiento de una Comisión Nacional de Ciberseguridad conformada por otros órganos cuya creación también propone, como la Conferencia de Ciberseguridad, la Agencia Nacional de Ciberseguridad, oficinas estatales de ciberseguridad y la Conferencia de Ciberdefensa. Esta última estaría integrada por elementos de la Secretaría de Defensa Nacional y Marina.

---

37. Artículo 52. Iniciativa presentada el 23 de marzo de 2021.

» Criminalización legal

Los bienes tutelados en los delitos incorporados atienden a naturalezas diversas, tales como: **a**) de los Delitos contra la confidencialidad, la Integridad y la disponibilidad de la Información; **b**) delitos contra el patrimonio; **c**) delitos contra la libertad de las personas; **d**) delitos a la propiedad intelectual; **e**) delitos contra la nación y **f**) delitos contra el Sistema Financiero. En el Anexo "Análisis de la Iniciativa de la Senadora Lucía Trasviña" se detalla el análisis desglosado de estos tipos penales. No obstante, a continuación ofrecemos una crítica general de los mismos:

Términos vagos y amplios. Estos tipos penales utilizan las expresiones "mediante cualquier medio o método" o "mediante el uso de equipos, sistemas o medios informáticos, electrónicos o telemáticos" para definir los medios a través de los cuales se cometerían estos delitos informáticos. Definir claramente los medios de comisión es crucial para una persecución penal efectiva, pues la falta de una definición clara de estos términos lleva a la criminalización de cualquier conducta legítima al usar herramientas tecnológicas.

Ausencia de elemento subjetivo y de daño. Expresiones como "sin autorización" o "sin causa legítima" utilizadas en algunos tipos penales para definir la intencionalidad no son claras. Esto provoca que la intencionalidad de cometer un delito sea difícil de delimitar y abarque a personas que no tenía intención de causar un daño.

Por su naturaleza, estos delitos deben ser dolosos y con la intención de causar un daño material. No definir claramente el elemento de intencionalidad puede criminalizar conductas legales en el entorno digital como la labor de periodistas o de investigadoras de seguridad informática.

Las personas investigadores de seguridad informática dedican su labor a explorar, analizar y arreglar las vulnerabilidades digitales que puedan encontrar en infraestructuras digitales. Realizan evaluaciones periódicas con distintos sistemas donde realizan pruebas de estrés para poder encontrar

vulnerabilidades en los sistemas. En caso de que las encuentren, las documentan, las comunican con las empresas responsables del producto y en algunos casos donde no se está haciendo público el riesgo, lo comunican a la sociedad.

Sin un elemento de intencionalidad claramente definido, las personas investigadores de seguridad tendrían un efecto inhibitorio a poder realizar su trabajo y compartir las vulnerabilidades encontradas con las empresas y la población en general[38].

Uno de los métodos utilizados son las "pruebas de penetración" o PEN testing, donde usan herramientas para para poder encontrar vulnerabilidades en sistemas, comunicar estos riesgos a quienes operan estos sistemas y poder prevenir ataques a tiempo. Muchas de estos tipos penales sancionan el uso y la simple posesión de este tipo de herramientas sin tener en cuenta la intención con la que se emplean.

De igual forma, la falta de elementos de intencionalidad y de daño también puede criminalizar conductas cometidas por error, como acceder o modificar un archivo por accidente. Sin el elemento de daño, se criminalizaría a una persona por un clic accidental que no causó un resultado material como pérdida de información o modificación irreparable de la información.

Es esencial establecer claramente la intencionalidad y el elemento de de daño de los tipos penales para evitar la penalización de estas conductas.

Criminalización de expresiones legítimas. Por su vaga redacción, los artículos 32 y 33 sobre incitación a la violencia e imagen personal criminalizan cualquier tipo de expresión o protesta que se pueda interpretar que incita a la violencia, como una sátira política.

---

38. Electronic Frontier Foundations. "Protecting Security Researchers' Rights in the Americas". 2018. Consulta en: https://www.eff.org/coders-rights-americas

Extender el alcance de los delitos sobre propiedad intelectual a todo uso de herramientas tecnológicas, sin delimitar propiamente los medios de comisión, puede criminalizar expresiones legítimas. Esta amplitud también puede criminalizar el uso legítimo de obras registradas bajo el derecho de autor. Esto resultaría en una criminalización y obstáculo a los derechos de acceso a la información, acceso a la cultura y educación.

Los delitos contra la Nación no delimitan excepciones que protejan la labor de periodistas e investigadoras de seguridad, lo cual puede criminalizar expresiones legítimas protegidas por la libertad de expresión. Esta falta de salvaguardas también criminaliza el derecho de acceso a la información. Es necesario crear tipos penales claros que contengan excepciones y salvaguardas adecuadas para proteger las expresiones legítimas y los derechos fundamentales.

Obstaculización de la persecución de delitos. Los tipos penales propuestos contienen redacciones tan amplias que pueden llevar a la confusión entre dichos delitos, lo cual también afectaría su efectiva persecución. Por ejemplo, en los delitos contra la Nación, los artículos 40 y 42 podrían tratarse del mismo delito, así como los artículos 44, 45 y 46.

Además, los tipos penales propuestos no proveen diferencia alguna con los tipos penales ya existentes en los códigos penales como los delitos de contra la intimidad sexual, trata de personas, pornografía infantil, delitos de propiedad intelectual, delitos contra la seguridad de la nación y delitos financieros que incluyen fraude y suplantación de identidad.

Por el contrario, generan una duplicación de delitos que complica la aplicación efectiva de las leyes penales y la persecución de delitos. Es necesario establecer tipos penales verdaderamente necesarios y evitar la inclusión de tipos penales ya existentes en las leyes aplicables para evitar la obstaculización de la persecución delictiva.

2) Iniciativa del Senador Miguel Ángel Mancera Espinosa (PRD)[39]

La iniciativa del senador propone una ley general con la finalidad de "proteger a las instituciones del Estado y a la sociedad frente a los ciberataques, lo anterior, a través de la instrumentación de acciones legislativas que permitan prevenir y sancionar los actos perpetrados por la ciberdelincuencia". Para ello propone contar con Comisión Permanente de Ciberseguridad dentro de la estructura del Consejo Nacional de Seguridad Pública, además de establecer delitos y mecanismos de coordinación internacional.

» Conceptos

Esta iniciativa también coloca el prejuicio de "ciber" para varias conductas realizables en otras esferas. El catálogo de conceptos es problemático porque contiene definiciones imprecisas que perciben la protección de sistemas informáticos principalmente desde la óptica del Estado.

Lo anterior puede propiciar una interpretación arbitraria de dichos conceptos. Esto implica que en la práctica existan actuaciones irregulares para la integración del delito desde la investigación o en la etapa judicial limitación de la aplicación de estándares en derechos humanos. Los comentarios específicos de estas definiciones se encuentran en el Anexo "Análisis de la Iniciativa del Senador Mancera".

» Competencia

El senador plantea una ley general para el funcionamiento de una política de ciberseguridad. Establece un Centro Nacional de Ciberseguridad, al cual le reconoce facultades como la prevención de delitos en contra de

---

39. Iniciativa del Senador Miguel Ángel Mancera Espinosa. http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf

la infraestructura de información crítica, la elaboración de la política de ciberseguridad del Estado y la autorización de prestadores de servicios de ciberseguridad.

» Participación de las fuerzas armadas

No identifica a ningún miembro de las fuerzas armadas en la vigilancia e investigación de los delitos propuestos. Sin embargo, faculta a un nuevo Centro Nacional de Ciberseguridad que emana del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública para la prevención de delitos.

» Criminalización legal

Los delitos propuestos comprenden: delitos contra la infraestructura de informática crítica, delitos contra de los sistemas informáticos, delitos contra las personas usuarias y delitos contra la ciberseguridad.

Esta iniciativa establece al Estado como principal sujeto pasivo y víctima de los tipos penales propuestos. La perspectiva de ciberseguridad desde la óptica del Estado y la falta de enfoque en las personas genera tipos penales que ponen en riesgo los derechos humanos. En el Anexo "Análisis de la Iniciativa del Senador Mancera" se detalla el análisis desglosado de estos tipos penales. No obstante, a continuación ofrecemos una crítica general de los mismos:

Términos vagos y amplios. Algunos tipos penales no especifican los medios para cometer los delitos y otros establecen que los delitos pueden cometerse "mediante cualquier medio" o incluso "mediante cualquier medio físico o electrónico", incluyendo la vía telefónica. Esto rebasa los alcances de una ley de en la materia al criminalizar el empleo de teléfonos.

Que no existan medios específicamente definidos para la comisión de delitos informáticos puede penalizar cualquier conducta que trastoque el entorno digital a través de cualquier medio.

Ausencia de elemento subjetivo y el elemento de daño. Expresiones contenidas en los tipos penales propuestos como "acceso sin autorización", "acceso de manera ilegítima" y afectación de sistemas "con ánimo de conseguir un lucro o provecho" son abstractas y no son suficientes para determinar si la persona tenía conocimiento o intención de cometer el delito. De igual forma, estos tipos penales carecen, en lo generalidad, de un elemento de daño que obligue a demostrar que existió un daño material para poder criminalizar la conducta.

Esto propicia la criminalización de conductas legítimas en el entorno digital. Por ejemplo, cualquier acceso a datos o sistemas, así como el ejercicio derecho de acceso a la información y la labor de periodistas, personas investigadoras de ciberseguridad y activistas. Por ello, como establecimos anteriormente, es necesario que el elemento de intencionalidad y de daño sea claro para evitar la penalización de estas conductas.

Criminalización de expresiones legítimas. El artículo 52[40] de la iniciativa criminaliza expresiones legítimas como parodias y críticas, pues penaliza la difusión de cualquier tipo de contenido, sin definir cuáles son constitutivos de delito, lo cual violenta la libertad de expresión. En caso de establecer tipos penales sobre contenido, es fundamental establecer claramente qué tipo de contenido sería constitutivo de delito, además de establecer excepciones y salvaguardas claras sobre el contenido amparado por la libertad de expresión.

---

40. Artículo 52.- A quien utilice el ciberespacio para publicar, almacenar y compartir contenidos que sean constitutivos de delitos, se le impondrán de 5 a 10 años de prisión sin perjuicio de las penas que les sean impuestas por la comisión de los delitos y multa que va de las 1000 a 2000 veces la unidad de medida y actualización vigentes al momento de la realización de la conducta. En aquellos casos en los que la información a la que se refiere el párrafo anterior sea constitutiva de delitos de pornografía o explotación de niñas, niños y adolescentes, las penas aumentarán hasta en dos terceras partes.

Obstaculización de la persecución de delitos. Como en la iniciativa anterior, el lenguaje de algunos tipos penales es tan similar que podría tratarse del mismo delito. Estas redacciones afectan el derecho de acceso a la información y criminalizan la labor de investigadoras de seguridad informática. Esto puede llevar a la confusión entre dichos delitos. Si bien la iniciativa deroga los artículos del Código Penal Federal[41] que se asimilan a los contenidos en esta iniciativa, la amplitud del alcance de estos tipos penales perjudica la efectiva persecución delictiva.

3) Iniciativa del Senador Gustavo Madero Múñoz (PAN)[42]

La iniciativa del senador propone reformar el Código Penal Federal, pues expone que es necesario actualizar el catálogo de delitos cibernéticos, con la finalidad de proteger la economía digital del Estado Mexicano.

» Conceptos

Al igual que las iniciativas antes expuestas, también existe una tendencia de colocar el prejuicio de "ciber" para varias conductas realizables en otras esferas. No obstante, a diferencia de las iniciativas analizadas, en esta el catálogo de palabras clave es reducido. Esto resulta problemático, pues dentro de las definiciones se refiere a redes o sistemas, conceptos que no fueron incorporados ni definidos en el mismo artículo. Los comentarios específicos a estas definiciones se encuentran en el Anexo "Análisis de la Iniciativa del Senador Madero".

---

41. Por ejemplo, los artículo 211 bis 1-5 que se asimilan a los delitos contra la infraestructura de información crítica, delitos contra los sistemas informáticos y delitos contra la ciberseguridad establecidos en la iniciativa.

42. Iniciativa del senador Gustavo Madero Muñoz: http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/03/asun_4161702_20210325_1613504011.pdf

» Competencia

Al ser una reforma al Código Penal Federal, la competencia es para la Fiscalía General de la República (FGR) y autoridades federales.

» Participación de las fuerzas armadas

No identifica a ningún miembro de las fuerzas armadas en la vigilancia e investigación de los delitos propuestos.

» Criminalización legal

Al ser una actualización, los delitos que se incorporan se ubican en el capítulo II Acceso ilícito a sistemas y equipos de informática, por lo que son conductas adicionales a las ya previstas. En el Anexo "Análisis de la Iniciativa del Senador Madero" se detalla el análisis desglosado de estos tipos penales. No obstante, a continuación ofrecemos una crítica general de los mismos:

Términos vagos y amplios. Los tipos penales propuestos no establecen medios de comisión. Como mencionamos anteriormente, en una ley de ciberseguridad es crucial establecer los medios utilizados para una persecución de delitos efectiva. Sin embargo, la falta de definición de los mismos propicia la arbitrariedad en la aplicación de la ley por parte de las autoridades.

Las expresiones "acceder de manera ilegítima", "sin derecho", "sin autorización" y "estando autorizado pero indebidamente [realice la conducta]" son muy generales. Esta imprecisión deriva en una ausencia del elemento de intencionalidad que resulta problemática para una aplicación efectiva de los tipos penales.

Ausencia de elemento subjetivo y de daño. Las expresiones mencionadas en el párrafo anterior no especifican si la persona tenía conocimiento o intención de cometer el delito. Esta ausencia de elemento subjetivo criminaliza conductas legales o conductas cometidas por error, lo cual convierte en ilícito el ejercicio de los derechos humanos.

Obstaculización de la persecución de delitos. El lenguaje de los tipos penales es tan similar que podrían ser el mismo delito. Estas redacciones amplias afectan el derecho de acceso a la información y la libertad de expresión; aunado a que criminalizan la labor de investigadoras de ciberseguridad.

E. RECOMENDACIONES GENERALES

Como hemos resaltado a lo largo del informe, el enfoque punitivista no sirve para afrontar los múltiples y diversos retos que existen en la política de ciberseguridad. Las personas legisladoras y creadores de política pública deben de centrarse en soluciones que efectivamente protejan a las personas en los entornos digitales.

Por lo cual, sugerimos las siguientes recomendaciones para las personas tomadoras de decisiones en materia de ciberseguridad y delitos informáticos.

1. Distinguir ciberseguridad de delitos informáticos. Comprender adecuadamente los alcances de la ciberseguridad y su diferencia con la creación de delitos informáticos. Esta distinción es vital para poder realizar decisiones de política pública que se centren efectivamente en atacar los problemas desde raíz y en proteger a las personas de manera más efectiva en línea y fuera de línea.

2. Poner a las personas como foco de protección. Establecer una política pública de ciberseguridad que se centre en proteger a las personas y sus derechos humanos. Es necesario que dicha estrategia parta de una óptica integral que vaya más allá de la criminalización de delitos informáticos y aborde la ciberseguridad desde la prevención, fortalecimiento de capacidades, establecimiento de políticas para reducir riesgos y mitigar daños en las infraestructuras de información.

3. Abstenerse de otorgar facultades a las fuerzas armadas. Las leyes de ciberseguridad deben abstenerse de otorgar facultades amplias a la Guardia Nacional y las fuerzas armadas. Esto implica prohibir que elementos militares puedan realizar intervención de comunica-

ciones, las solicitudes para bajar contenido, el acceso a datos conservados, entre otras prácticas. Este tipo de medidas son sumamente invasivas en la privacidad de las personas por lo cual no pueden recaer en elementos de las fuerzas armadas.

4. Atender a los principios constitucionales en materia penal. Los principios de mínima intervención, derecho penal de acto y taxatividad[43] deben ser respetados a fin de establecer tipos penales claros, precisos y exactos para evitar confusiones en su aplicación.

5. Establecer tipos penales verdaderamente necesarios. Esto evitará catálogos extensos de tipos penales que criminalicen expresiones legítimas o el ejercicio de los derechos humanos. También evitará la obstaculización de la persecución delictiva generada por la confusión que provoca la inclusión de tipos penales ya existentes en las leyes aplicables.

6. Incluir salvaguardas y excepciones que protejan el ejercicio de los derechos humanos. Es esencial incluir excepciones que amparen el derecho de acceso a la información, la protección de datos personales, la privacidad, la libertad de expresión, el acceso a las TIC, entre otros derechos. Es necesario establecer excepciones que protejan expresamente la labor de periodistas, activistas e investigadoras de ciberseguridad. Esto asegurará la constitucionalidad y operatividad de una ley en la materia.

7. Cualquier intervención de las comunicaciones siempre debe contar con la salvaguardas suficientes para poder prevenir abusos que resulten en violaciones de derechos humanos.

---

43. Estos principios se describen en el apartado Derecho Penal y Teoría del Delito del presente informe.La UNODA es un organismo de la Secretaría General de la ONU que se encarga del desarme nuclear y la no proliferación. Además, fortalece los mecanismos para que se logre el objetivo principal de reducir las cantidades existentes de los diferentes tipos de armamento, que pueden ser, de destrucción masiva o convencional.

8. Definir claramente los medios de comisión de los tipos penales. Para una persecución penal efectiva es crucial establecer claramente los medios utilizados para cometer delitos informáticos, pues la falta de una definición clara de estos términos puede llevar a la criminalización de cualquier conducta legítima al usar herramientas tecnológicas.

9. Establecer claramente la intencionalidad de los tipos penales. Esto evitará la criminalización de conductas legítimas en el entorno digital, como la labor de periodistas, activistas o investigadoras de investigación que utilizan herramientas tecnológicas para desempeñar sus funciones. De igual forma, evitará la criminalización de conductas realizadas por error.

10. Definir conceptos esenciales y evitar uso excesivo del prefijo "ciber". Es necesario incluir definiciones de cuestiones básicas en materia de ciberseguridad como redes, sistemas, datos o infraestructuras críticas de información para asegurar un entendimiento común de dichos conceptos que permita la aplicación efectiva de la ley. Es importante abstenerse de agregar el prefijo ciber a conductas realizables en otras esferas para evitar definiciones discrepantes.

11. Establecer terminología clara, precisa y exacta. Estas definiciones atiendan a una perspectiva de derechos humanos y no perciban la protección de sistemas informáticos únicamente desde la óptica del Estado. Esto implica, por ejemplo, incluir definiciones que atiendan a la protección de datos personales y a la difusión de contenido en el ejercicio de la libertad de expresión.

12. Incluir a la sociedad civil de manera proactiva y transparente. Además de otras partes interesadas como el sector privado y académico, es necesario incorporar organizaciones de la sociedad civil especializadas en derechos digitales, derechos de la niñez, derechos de las mujeres, derechos humanos en el ámbito penal, entre otras. La diversidad de los actores y una efectiva rendición de cuentas en la toma de decisiones permitirá la presentación de una iniciativa operativa y constitucionalmente viable.

III. ANEXOS

I.ELEMENTOS DEL DELITO

ELEMENTO	DEFINICIÓN
CONDUCTA	Acción u omisión. Comportamiento humano voluntario, que se puede manifestar con el hacer (positivo) o no hacer (negativo), encaminado a un propósito.
TIPICIDAD	Es la adecuación exacta de la conducta realizada al tipo penal previamente descrito
ANTIJURIDICIDAD	Es el juicio de valor objetivo que se realiza a la conducta descrita que lesiona o pone en peligro un derecho.
PUNIBILIDAD	Es la amenaza de sanción establecida en el tipo penal por la comisión del delito.
CULPABILIDAD	Es el reproche que se le realiza a la persona con consciencia sobre la existencia de conductas delictivas de no haber evitado su realización. Su manifestación puede ser de manera intencional (dolosa) o imprudencial (culposa).

NO SE ACTUALIZA CUANDO

- Sonambulismo.
- Fuerza mayor.
- Causas de la naturaleza.
- Hipnotismo.

- Falta de calidad de las personas que intervinieron en la conducta.
- Falta de presupuestos del delito.
- Falta de medios comisivos.
- Falta de alguno de los elementos del tipo penal.
- Consentimiento de la víctima que recaiga sobre algún bien jurídico disponible.

- Consentimiento presunto.
- La legítima defensa.
- El estado de necesidad.
- Ejercicio de un derecho.
- Cumplimiento de un deber.

- Los códigos Penales establecerán en qué hechos no se aplicará sanción. De acuerdo a la política criminal no se considera pertinente imponer sanción.

- *Errores.* de prohibición, hecho, objeto.
- No exigibilidad de otra conducta.
- Existe inculpabilidad cuando la persona que comete la conducta lo realiza bajo ignorancia o error imposible de vencer.

II. ANÁLISIS DE LA INICIATIVA DE LA SENADORA LUCÍA TRASVIÑA

CONCEPTOS Y TIPOS PENALES DESCRITOS EN LA INICIATIVA DE LA SENADORA LUCÍA TRASVIÑA

ELEMENTO	DEFINICIÓN
CIBERAMENAZA	Riesgo potencial relacionado a las vulnerabilidades de los sistemas informáticos e infraestructura física y pasiva de las redes públicas de telecomunicaciones de permitir causar daño a los procesos y continuidad de las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.
CIBERATAQUE	Acción realizada a través de las redes de telecomunicaciones con el objetivo de dañar las Infraestructuras Críticas de Información, las Infraestructuras de Información Esenciales, así como la seguridad de las personas.
CIBERDEFENSA	Conjunto de acciones, recursos y mecanismos del estado en materia de seguridad nacional para prevenir, identificar y neutralizar toda ciber-amenaza o ciber-ataque que afecte a la infraestructura crítica nacional.
CIBERDELINCUENCIA	Actividades que llevan a cabo individuo(s) realiza(n) en el que utilizan como medio o como fin a las Tecnologías de la Información y Comunicación.

COMENTARIOS

» La definición es peligrosa porque no delimita lo que es "riesgo" y cómo se presenta de manera potencial, de dónde puede presentarse, tampoco lo referente a "amenaza", pues sólo parte desde el riesgo, el cual tampoco establece si este debe ser inminente, el periodo de vigencia ni el tipo de daño.

» Es un concepto que parte de ponderar la "amenaza" desde la mirada de afectación del estado, dejando relegado los intereses de las personas hacia un posible riesgo o vulneración.

» Debe ser una conducta de hacer, no permite o acepta una omisión, por ende, es una acción dolosa. No especifica qué tipo de ataque.

» Permite la intromisión y fiscalización del estado en las actividades digitales de las personas debido a la "prevención de una crítica nacional".

» Esta definición es imprecisa, pues crea confusión en términos de la autoría y participación del delito, así como de lo establecido en la ley respecto a pandilla y delincuencia organizada.

CIBERESPACIO	Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico.
CIBERSEGURIDAD	Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.
DELITOS CIBERNÉTICOS/ CIBERDELITOS	Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional.
ACTIVO	Se refiere a información, procesos, personas y tecnología que aporta valor y son relevantes para el objeto principal de una empresa, Institución, así como datos personales.
ALGORITMO	Conjunto ordenado de operaciones o funciones matemáticas que permite solucionar un determinado problema o lograr un resultado definido.
APLICACIÓN	Programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas. Esto lo diferencia principalmente de otros tipos de programas, como los sistemas operativos, las utilidades, y las herramientas de desarrollo de software.
AUTENTICACIÓN	Procedimiento para comprobar que alguien es quien dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

» No precisa la competencia del estado mexicano en la investigación y vigilancia de la actividad digital de las personas usuarias de internet.

» Subscribe las acciones de monitoreo, protección, prevención e investigación de hechos delictivos a un rubro de seguridad nacional, lo que abre la posibilidad de intervención de elementos de las fuerzas armadas y otras medidas más intransigentes.

» Esta definición es sumamente problemática, debido a que a pesar que la iniciativa plantea una ley general con descripciones delictivas, al señalar a las tecnologías de la información y comunicación como medios o fin de los delitos que se encuentren tipificados en "algún" código penal u otro ordenamiento, permite que cualquier delito sea un delito cibernético, lo que hace innecesario contar con una ley general.

» Este concepto se relaciona con el de Activo virtual, que es la representación en valor registrado electrónicamente y utilizado entre el público como medio de pago para todo tipo de actos jurídicos, cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos. Los cuales se encuentran sujetos a la normativa que el Banco de México formule. Es una definición inespecífica.

» No especifica qué es conjunto, cuáles son las operaciones matemáticas, qué problema determinado y cuál es el resultado definido.

» Definición muy general.

» Existen otros métodos como la verificación, que son menos invasivos para lograr comunicaciones seguras.

AUTENTICIDAD	O no repudio, constituye un pilar de la seguridad de la información, el cual consiste en la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.
DOMINIO	Espacio de aplicabilidad intangible que define el campo de acción del ciberdelito.
ARCHIVO INFORMÁTICO	Conjunto organizado de unidades de información (bits) almacenados en un dispositivo electrónico el cual puede ser modificado o asignado a voluntad del usuario o del programador, y que contiene un nombre y extensión que determina qué tipo de archivo es y qué funciones cumple.
BORRADO SEGURO	Proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
DATOS BIOMÉTRICOS	Cualquier registro o dato que hace referencia al reconocimiento de personas basado en sus características fisiológicas como el ADN (ácido desoxirribonucleico), huellas dactilares, retina, iris de los ojos, patrones faciales o de voz, así como las medidas de las manos a efectos de autenticación de identidad.
DATOS INFORMÁTICOS	» Representación simbólica mediante números o letras de una recopilación de información, la cual puede ser cualitativa o cuantitativa que faciliten la deducción de un hecho. » Es toda aquella representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

» Este concepto se denomina igual a otro que se contempla en el listado, el cual también se encuentra relacionado con la validez de la información en tiempo, forma y distribución, también con la garantía que el origen de la información para evitar la suplantación de identidades.

» No cumple con los requisitos de validez espacial de la ley penal que delimita el alcance de aplicación territorial de la norma penal.

» Otra definición que describe, que crea relación o cercanía con el concepto de Base de Datos, que se considera una colección de datos o información relacionados entre sí que tienen un significado implícito.

» La definición no identifica en dónde se encuentra lo seguro.

» No es clara la necesidad de definir conceptos que corresponden a las leyes de datos personales.

» Además, mezcla el concepto de datos genéticos con el de datos biométricos, lo cual puede intervenir negativamente en la aplicación de la ley.

» Entremezcla conceptos distintos.

DISPOSITIVO	Aparato, artificio, mecanismo, artefacto, órgano, periférico, gadget, producto, elemento de un sistema o componente electrónico
DISPOSITIVO DE ACCESO	Es toda tarjeta, placa, código, número, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes.
RECONOCIMIENTO BIOMÉTRICO	Identificación o verificación de la identidad de una persona a partir de la comparación de plantillas biométricas.

» Definición muy general. Esto puede intervenir negativamente en la aplicación de la ley.

» Definición muy general. Esto puede intervenir negativamente en la aplicación de la ley.

» No es clara la necesidad de definir conceptos que corresponden a las leyes de datos personales.

» Entremezclar la identificación biométrica con la verificación biométrica en una misma definición, sin marcar su diferencia es riesgoso para los derechos humanos que se pueden ver involucrados con las tecnologías de RF.

» La identificación es un método más invasivo, por lo que no marcar la diferencia provoca que no se establezcan los controles necesarios para el despliegue de esta tecnología.

DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LA INFORMACIÓN

Elemento normativo

Artículo 24. Acceso ilícito a tecnologías de la información y comunicaciones, sistemas informáticos, electrónicos o telemáticos.
Artículo 26. Interceptación e Intervención de Datos o Señales.
Artículo 27. Falsificación informática.
Artículo 28. Abuso de Dispositivos Tecnológicos.

Elementos objetivos o descriptivos

CONDUCTA	Acceder, interceptar, intervenir, utilizar, poseer, vender, obtener o distribuir, entre otros.
TIPO DE RESULTADO	Estos tipos penales son de resultado material; es decir, se le debe atribuir una acción u omisión que realiza la persona activa del delito. Estos tipos penales no identifican supuestos de tentativa punible, por lo que debemos recurrir a lo que establece el artículo 12 del Código Penal Federal (CPF).
BIEN JURÍDICO TUTELADO	Confidencialidad, integridad y disponibilidad de la información de personas físicas, morales y del estado.
PERSONA ACTIVA	En estas descripciones puede ser cualquier persona la que despliega la conducta. Como estos tipos penales no hacen mención de ello, debemos acudir a lo establecido en el artículo 13 del CPF, que identifica la autoría y participación.
PERSONA PASIVA	No lo especifica. Puede ser cualquier persona la que recibe la puesta en peligro o la lesión de sus bienes jurídicos y derechos.

MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» En estos delitos se requiere acreditar los medios que utilizó la persona activa para causar la lesión o puesta en peligro del bien jurídico, es decir, advertir la existencia del nexo causal. » *Términos vagos y amplios*. La expresión "cualquier medio o método" es muy amplia y puede criminalizar cualquier conducta legítima al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Se cometan en perjuicio de propiedades del Estado. » *Ocasión.* Cuando el acceso no autorizado sea para la clonación, venta, distribución o cualquier otra utilización de un dispositivo de acceso a un servicio o sistema informático, electrónico o de telecomunicaciones.

Elemento subjetivo

ELEMENTO SUBJETIVO	» Atiende al estado de conciencia, voluntad o afectividad de la persona activa. » Estos tipos penales deben ser dolosos; es decir, la persona activa debe actuar teniendo conocimiento y voluntad de llevar a cabo las conductas determinadas. » *Términos vagos y amplios.* Pese a lo anterior, las expresiones "sin autorización" o "sin causa legítima" no son claras y hacen que la intencionalidad sea difícil de delimitar. La falta de especificaciones respecto a la intencionalidad puede criminalizar conductas legales como la labor de periodistas o de investigadoras de seguridad, así como conductas cometidas por error.

DELITOS CONTRA EL PATRIMONIO

Elemento normativo

Artículo 29. Fraude por medio informático.

Elementos objetivos o descriptivos

CONDUCTA	Engañar o aprovecharse para obtener un beneficio patrimonial.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Bienes o derechos patrimoniales de personas físicas, morales y del estado.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* La expresión "cualquier medio o método" es muy amplia y puede criminalizar cualquier conducta legítima al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» No tiene.

Elemento subjetivo

ELEMENTO SUBJETIVO	» Tipo penal doloso.

DELITOS CONTRA LA LIBERTAD DE LAS PERSONAS

Elemento normativo

Artículo 30. Acceso y uso indebido de datos personales.
Artículo 31. Usurpación de identidad.
Artículo 32. Incitación a la Violencia y Alteración del Orden Social.
Artículo 33. Delitos contra la Imagen Personal.

Elementos objetivos o descriptivos

CONDUCTA	Obtener, almacenar, sustraer, ofrecer, vender, enviar, entre otros, datos personales. Apropiarse de un medio de identificación de otra persona. Describir, diseñar, grabar material que incite a la violencia.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Datos personales, identidad, imagen.
PERSONA ACTIVA	Sólo el delito de imagen personal especifican quién se considera persona activa.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Término vagos y amplios.* La expresión "producto de la evolución tecnológica" es muy amplia y puede criminalizar cualquier conducta legítima al usar herramientas tecnológicas.

CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN

» *Agravante.* La realización de transacciones comerciales que afecte derechos individuales o patrimoniales de la víctima.

» *Modo.* Conducta sea reiterada ante una misma o en diferentes instancias bancarias.

» *Ocasión.* Si una de las partes involucradas laboró o formó parte de algunas de las instancias bancarias.

» *Personal.* Exista relación de cónyuge, concubina o concubinario, o la persona que mantenga o haya mantenido una relación sentimental, etc.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Ausencia de elemento subjetivo.* La redacción del artículo 30 es tan amplia criminaliza conductas realizadas por error, por ejemplo, abrir un archivo por accidente. Los artículos 32 y 33 tampoco incluyen un elemento claro de intencionalidad, por lo que también podrían criminalizar conductas legales o conductas cometidas por error.

» *Criminalización de expresiones legítimas.* Los artículos 32 y 33 son tan vagos que penalizan cualquier tipo de expresión o protesta que se pueda interpretar que incita a la violencia, como una sátira política.

DELITOS SEXUALES

Elemento normativo

Artículo 34. Pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o que no tienen capacidad para resistirlo.
Artículo 35. Seducción de menores a través de medios informáticos o digitales de la Internet o por medios electrónicos.
Artículo 36. Turismo Sexual.
Artículo 37. Lenocinio a través del uso de las tecnologías de información y comunicación.

Elementos objetivos o descriptivos

CONDUCTA	Divulgar, distribuir, comercializar contenido sexual. Solicitar, procurar, promover, almacenar, entre otros, pornografía de menores.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Desarrollo psicoemocional y sexual de niñez, adolescencia y personas adultas.
PERSONA ACTIVA	Los delitos de seducción de menores, lenocinio especifican quién se considera persona activa.
PERSONA PASIVA	Sólo los delitos sexuales contra personas menores de dieciocho años de edad o de personas vulnerables especifican que éstas son la persona pasiva.

MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* "A través de anuncios impresos, sistemas informáticos, electrónicos, telemáticos, programas o aplicaciones que sean fruto de la evolución tecnológica" es muy amplia y rebasa el alcance de una legislación en materia de ciberseguridad al establecer anuncios impresos como medios de comisión.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* La pena aumenta en una mitad si se hiciere uso de violencia física o moral o psicoemocional, o se aproveche de la ignorancia, extrema pobreza o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse.

Elemento subjetivo

ELEMENTO SUBJETIVO	» Estos tipos penales son dolosos. Sin embargo, de las redacciones no se aprecia un elemento de intencionalidad, por lo que existe una ausencia de elemento subjetivo criminaliza conductas legales o conductas cometidas por error.

DELITOS CONTRA LA PROPIEDAD INTELECTUAL

Elemento normativo

Artículo 39. Delitos de la Ley Federal de Derechos de Autor y la Ley de Propiedad Industrial.

Elementos objetivos o descriptivos

CONDUCTA	No la especifica.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Protección para todo creador de obras literarias o artísticas.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* "a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o en cualquiera de sus componentes" es muy amplia y puede criminalizar cualquier conducta legítma al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» No tiene.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Ausencia de elemento subjetivo.* No especifica intencionalidad. La referencia a los delitos contenidos en otras leyes es errónea ya que la LFDA no establece delitos en materia de derecho de autor, sino el CPF.

» Extender el alcance de los delitos sobre propiedad intelectual a todo uso de herramientas tecnológicas, sin delimitar propiamente los medios de comisión puede criminalizar expresiones legítimas.

» También puede criminalizar todo acceso a material protegido por la propiedad intelectual en el entorno digital, lo cual violenta el derecho de acceso a la cultura y el derecho a la educación.

DELITOS CONTRA LA NACIÓN

Elemento normativo

Artículo 40. Delitos contra la nación.
Artículo 41. Delitos contra la seguridad nacional.
Artículo 42. Delitos de los servidores públicos.

Elementos objetivos o descriptivos

CONDUCTA	Copiar extraer, alterar, eliminar, entre otros, dolosamente información relacionada con infraestructuras críticas del Estado. Poner en peligro o afectar información o funcionalidad de infraestructuras críticas de la información.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	La seguridad nacional.
PERSONA ACTIVA	Sólo lo especifica en los delitos de servidores públicos.
PERSONA PASIVA	El Estado Mexicano.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* Las expresiones "por cualquier medio o método" y "mediante el uso de equipos, sistemas o medios informáticos, electrónicos o telemáticos" son muy amplias y pueden criminalizar cualquier conducta legítma al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Servidor o ex servidor público. A quien aprovechándose de los conocimientos especializados en materia de tecnologías de la información y comunicación, realice alguna de las conductas.

Elemento subjetivo

ELEMENTO SUBJETIVO

» El artículo 42 es un tipo penal doloso.

» *Ausencia de elemento subjetivo.* La expresión "sin autorización" del art. 40 es abstracta y no especifica si la persona tenía conocimiento o intención de cometer el delito. Esto criminaliza conductas legales o conductas cometidas por error.

» No delimita excepciones que protejan la labor de periodistas e investigadoras de seguridad, lo cual puede *criminalizar expresiones legítimas*, la libertad de expresión y el derecho de acceso a la información.

» Los artículos 40 y 42 podrían ser el mismo tipo penal, lo cual *obstaculiza la persecución de delitos.*

DELITOS CONTRA EL SISTEMA FINANCIERO

Elemento normativo

Artículo 44.
Artículo 45.
Artículo 46.

Elementos objetivos o descriptivos

CONDUCTA	Poner en peligro, dañar, alterar, obstaculizar, destruir el funcionamiento de sistemas o medios informáticos de instituciones financieras.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	El debido funcionamiento del sistema financiero mexicano.
PERSONA ACTIVA	Sólo lo especifica en las agravantes.
PERSONA PASIVA	Instituciones del sistema financiero.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* La expresión "por cualquier medio o método" es muy amplia y puede criminalizar cualquier conducta legítma al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Cuando el delito lo comentan empleados o ex empleados de instituciones financieras o de prestadoras de servicios a instituciones públicas y financieras. Cuando hayan firmado un acuerdo de confidencialidad.

Elemento subjetivo

ELEMENTO SUBJETIVO

» Los artículos 44 y 45 son dolosos.

» *Términos vagos y amplios.* La expresión "obtenga ilícitamente un beneficio patrimonial, económico o de otra naturaleza para sí o para un tercero" es vaga y es insuficiente para definir la intencionalidad de la conducta, por lo que existe una *ausencia de elemento subjetivo* que podría criminalizar conductas legales o conductas cometidas por error.

» *Obstaculización de persecución de delitos.* Las redacciones son tan similares que podrían ser el mismo delito. Además, criminalizan cualquier acceso a información realizado por un empleado de instituciones financieras en el ejercicio de sus funciones.

II. ANÁLISIS DE LA INICIATIVA DEL SENADOR MIGUEL ÁNGEL MANCERA

CONCEPTOS Y TIPOS PENALES DESCRITOS EN LA INICIATIVA DEL SENADOR MIGUEL ÁNGEL MANCERA

CONCEPTO	DEFINICIÓN
CIBERATAQUE	Acción realizada a través de uno o varios sistemas informáticos con el objeto de amenazar, afectar, inhabilitar, destruir, vulnerar, eliminar, negar o modificar la información contenida en un sistema de información, bases de datos y/o registro digital.
CIBERAMENAZA	Cualquier situación potencial, hecho o acción que pueda amenazar, dañar, eliminar, modificar, perturbar, negar o afectar desfavorablemente de otra manera las redes y los sistemas de información, a las personas usuarias de tales sistemas y a otras personas que puedan resultar afectadas.
CIBERDEFENSA	Conjunto de acciones, recursos y mecanismos en materia de seguridad para prevenir, identificar, reaccionar y neutralizar las amenazas, ciberamenazas o ciberataques.
CIBERDELINCUENCIA	Actividades que llevan a cabo individuo(s) realiza(n) en el que utilizan como medio o como fin a las Tecnologías de la Información y Comunicación.

COMENTARIOS

» Debe ser una conducta de hacer, no permite o acepta una omisión, por ende, es una acción dolosa. No especifica qué tipo de ataque. No delimita una intención de daño, lo cual amplía el alcance de la definición. La definición es peligrosa porque coloca en el mismo nivel la "amenaza" como una conducta que pone en riesgo con "destruir" que ya es una conducta consumada.

» La definición es peligrosa porque coloca en el mismo nivel la "amenaza" como una conducta que pone en riesgo con "dañar" que ya es una conducta consumada.

» Es un concepto que parte de ponderar la "amenaza" desde la mirada de afectación del Estado, dejando relegado los intereses de las personas hacia un posible riesgo o vulneración.

» Permite la intromisión y fiscalización del Estado en las actividades digitales de las personas debido a la "prevención de una crítica nacional".

» Esta definición es imprecisa, pues crea confusión en términos de la autoría y participación del delito, así como de lo establecido en la ley respecto a pandilla y delincuencia organizada. Bajo esta definición, cualquier conducta en el entorno digital podría ser criminalizada.

CIBERESPACIO	Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas, empresas, todos los órdenes de gobierno, dispositivos electrónicos y sistemas informáticos.
CIBERSEGURIDAD	Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación.
RIESGO	La posibilidad de que una ciberamenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los sistemas informáticos, la información contenida en estos o las infraestructuras críticas.
SISTEMA INFORMÁTICO	Todo dispositivo o conjunto de dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el procesamiento de datos digitales.
VULNERABILIDADES	Las características o defectos de un sistema informático que pueden ser utilizadas o explotadas por una o más ciberamenazas.

» No precisa la competencia del Estado Mexicano en la investigación y vigilancia de la actividad digital de las personas usuarias de internet.

» Subscribe las acciones de monitoreo, protección, prevención e investigación de hechos delictivos a un rubro de seguridad nacional, lo que abre la posibilidad de intervención de elementos de las fuerzas armadas y otras medidas más intransigentes.

» La definición es peligrosa porque no delimita lo que es "riesgo" y cómo se presenta de manera potencial, de dónde puede presentarse, tampoco lo referente a "amenaza", pues sólo parte desde el riesgo, el cual tampoco establece si este debe ser inminente, el periodo de vigencia ni el tipo de daño.

» Definición muy general.

» Al tener una definición deficiente de amenaza, es riesgoso definir las vulnerabilidades a partir de este concepto.

DELITOS CONTRA LA INFRAESTRUCTURA DE INFORMÁTICA CRÍTICA

Elemento normativo

Artículo 39.
Artículo 40.
Artículo 41.

Elementos objetivos o descriptivos

CONDUCTA	Vulnerar, inhabilitar, robar, intervenir, destruir o afectar, copiar, modificar, limitar el acceso, corromper, destruir, entre otros.
TIPO DE RESULTADO	Estos tipos penales son de resultado material; es decir, se le debe atribuir una acción u omisión que realiza la persona activa del delito. Estos tipos penales no identifican supuestos de tentativa punible, por lo que debemos recurrir a lo que establece el artículo 12 del Código Penal Federal (CPF).
BIEN JURÍDICO TUTELADO	Confidencialidad, integridad y disponibilidad de la información de personas físicas, morales y del estado.
PERSONA ACTIVA	En estas descripciones puede ser cualquier persona la que despliega la conducta, por lo que debemos acudir a lo establecido en el artículo 13 del CPF, que identifica la autoría y participación. Sólo especifica el sujeto activo en el caso de agravantes.
PERSONA PASIVA	En estas descripciones puede ser cualquier persona la que recibe la puesta en peligro o la lesión de sus bienes jurídicos y derechos. Sin embargo, esta iniciativa pone al Estado como principal persona pasiva y víctima de los delitos.

MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» En estos delitos se requiere acreditar los medios que utilizó la persona activa para causar la lesión o puesta en peligro del bien jurídico; es decir, advertir la existencia del nexo causal. » Estos tipos penales no especifican el medio.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Cuando la persona que realice la conducta se encuentre a cargo, controle u opere la infraestructura objeto de esta conducta, se le aumentará la pena hasta en una mitad. Cuando se trate de persona servidora pública se le aumentará la pena en una mitad.

Elemento subjetivo

ELEMENTO SUBJETIVO	» Atiende al estado de conciencia, voluntad o afectividad de la persona activa. Estos tipos penales deben ser dolosos; es decir, la persona activa debe actuar teniendo conocimiento y voluntad de llevar a cabo las conductas determinadas. » *Términos vagos y amplios.* Las expresiones "acceder de manera ilegítima" o "sin autorización" son abstractas. » No incluye un elemento de intencionalidad; es decir, no especifican si la persona tenía conocimiento o intención de cometer el delito. *Esta ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error. » *Obstaculización de persecución de delitos.* El lenguaje de los tipos penales es tan similar que podrían ser el mismo delito. » Estas redacciones afectan el derecho de acceso a la información y criminalizan la labor de investigadoras de seguridad informática.

DELITOS EN CONTRA DE LOS SISTEMAS INFORMÁTICOS

Elemento normativo

Artículo 42.
Artículo 43.
Artículo 44.
Artículo 45.
Artículo 46.
Artículo 47.

Elementos objetivos o descriptivos

CONDUCTA	Acceder, obtener, copiar, corromper, limitar, modificar, destruir y chantajear.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Confidencialidad, integridad y disponibilidad de la información de personas físicas, morales y del estado.
PERSONA ACTIVA	Cualquier persona, incluyendo a quien actúe por encargo.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» Estos tipos penales no especifican el medio.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Contenido íntimo, datos personales.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Términos vagos y amplios.* La expresión "sin autorización" es abstracta y no especifica si la persona tenía conocimiento o intención de cometer el delito.

» Esta ausencia de *elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

» Así mismo, estas redacciones amplias afectan el derecho de acceso a la información y criminalizan la labor de investigadoras de seguridad informática.

DELITOS CONTRA LAS PERSONAS USUARIAS

Elemento normativo

Artículo 48.
Artículo 49.
Artículo 50.
Artículo 51.
Artículo 52.

Elementos objetivos o descriptivos

CONDUCTA	Acceder, suplantar, simular, crear, capturar, grabar, copiar, alterar, duplicar, clonar, eliminar, publicar, almacenar y compartir.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Datos personales, identidad, imagen.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* La expresión "de manera física o a través de otro u otros sistemas informáticos y por cualquier medio" es muy amplia y puede criminalizar cualquier conducta legítima al usar herramientas tecnológicas.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Datos personales o bancarios.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Términos vagos y amplios.* "Al que acceda de manera ilegítima a uno o más sistemas informáticos", "A quien intencionalmente y sin la debida autorización por cualquier medio" y "A quien utilice el ciberespacio para..." son abstractas y no especifican si la persona tenía conocimiento o intención de cometer el delito.

» Esta *ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

» Además, la amplitud de las redacciones afecta el derecho de acceso a la información al criminalizar cualquier tipo de acceso a datos.

» El art. 52 *criminaliza* expresiones legítimas como parodias y críticas, pues penaliza la difusión de cualquier tipo de contenido, sin definir cuáles son constitutivos de delito.

DELITOS CONTRA LA CIBERSEGURIDAD

Elemento normativo

Artículo 53.
Artículo 54.
Artículo 55.
Artículo 56.

Elementos objetivos o descriptivos

CONDUCTA	Hacer, distribuir, utilizar, afectar.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Debido funcionamiento de infraestructuras críticas, seguridad nacional.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	El único sujeto pasivo claro es el Estado.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» *Términos vagos y amplios.* Sólo especifica los medios en el delito en contra del Estado, donde dice que se puede cometer "por vía telefónica, comunicación electrónica o cualquier medio físico o electrónico". Esta redacción es muy amplia y puede criminalizar cualquier conducta al usar herramientas tecnológicas. » Incluso, rebasa los alcances de una ley de ciberseguridad al criminalizar el empleo de teléfonos, lo cual genera una *obstaculización de persecución de delitos.*

CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN

» *Agravante.* Sistemas informáticos considerados infraestructura informática crítica.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Términos vagos y amplios.* Las expresiones "A quien lleve a cabo modificaciones no autorizadas", "A quien utilice sistemas informáticos de manera parcial o total, con autorización o sin ella", "con ánimo de conseguir un lucro o provecho" son abstractas y no especifican si la persona tenía conocimiento o intención de cometer el delito.

» Esta *ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

II. ANÁLISIS DE LA INICIATIVA DEL SENADOR GUSTAVO MADERO MÚÑOZ

CONCEPTOS Y TIPOS PENALES DESCRITOS EN LA INICIATIVA DEL SENADOR MADERO

CONCEPTO	DEFINICIÓN
CIBERATAQUE	Cualquier acto u omisión cuyo objetivo sea infiltrar, sin autorización, redes de telecomunicaciones, redes públicas de telecomunicaciones, sistemas de información o equipos informáticos.
CIBERAMENAZA	Cualquier situación potencial, hecho o acción que pueda dañar, perturbar o afectar las redes de telecomunicaciones, redes públicas de telecomunicaciones y los sistemas de información, a los usuarios de tales sistemas.
CIBERSEGURIDAD	Toda acción tendiente a proteger las redes de telecomunicaciones, redes públicas de telecomunicaciones y sistemas de información, de los usuarios de tales sistemas, sean públicos o privados, afectadas por las ciberamenazas.
SISTEMA INFORMÁTICO	Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.
INTERNET	Lo que establece el artículo 3, fracción XXXII de la Ley Federal de Telecomunicaciones y Radiodifusión.
REDES DE TELECOMUNICACIONES	Lo que establece el artículo 3, fracción XXXII de la Ley Federal de Telecomunicaciones y Radiodifusión.
REDES PÚBLICAS DE TELECOMUNICACIONES	Lo que establece el artículo 3, fracción XXXII de la Ley Federal de Telecomunicaciones y Radiodifusión.

COMENTARIOS

» Debe ser una conducta de hacer, no permite o acepta una omisión, por ende, es una acción dolosa. No especifica qué tipo de ataque.

» Al señalar "cualquier situación potencial, hecho o acción", no identifica la conducta sancionable. Tampoco indica qué son las redes públicas o sistemas de telecomunicación.

» Esta definición es peligrosa debido a que se criminaliza el uso de internet al señalar que la ciberseguridad son acciones tendientes a proteger las redes de los usuarios.

» Definición ambigua.

» Esto resulta confuso para la consulta de personas no abogadas.

» Esto resulta confuso para la consulta de personas no abogadas.

» Esto resulta confuso para la consulta de personas no abogadas.

DELITOS CONTRA LAS REDES DE TELECOMUNICACIONES

Elemento normativo

Artículo 211 bis 2.
Artículo 211 bis 3.
Artículo 211 bis 6.

Elementos objetivos o descriptivos

CONDUCTA	» *Artículo 211 bis 2.* Vulnerar, inhabilitar, robar información, intervenir, destruir o afectar redes de telecomunicaciones, redes públicas de telecomunicaciones y sistemas de información. » *Artículo 211 bis 3.* Acceda, intervenga u obstaculice total o parcialmente los servicios prestados por internet. » *Artículo 211 bis 6.* Infiltrar redes de telecomunicaciones, redes públicas de telecomunicaciones o sistemas informáticos.
TIPO DE RESULTADO	Estos tipos penales son de resultado material; es decir, se le debe atribuir una acción u omisión que realiza la persona activa del delito. Estos tipos penales no identifican supuestos de tentativa punible, por lo que debemos recurrir a lo que establece el artículo 12 del Código Penal Federal (CPF).
BIEN JURÍDICO TUTELADO	Servicios de telecomunicaciones.
PERSONA ACTIVA	En estas descripciones puede ser cualquier persona la que despliega la conducta, por lo que debemos acudir a lo establecido en el artículo 13 del CPF, que identifica la autoría y participación.

PERSONA PASIVA	En estas descripciones puede ser cualquier persona la que recibe la puesta en peligro o la lesión de sus bienes jurídicos y derechos. Dada la naturaleza de estos tipos penales, puede ser cualquier persona física, moral o el Estado que administre redes de telecomunicaciones.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» En estos delitos se requiere acreditar los medios que utilizó la persona activa para causar la lesión o puesta en peligro del bien jurídico; es decir, advertir la existencia del nexo causal. Estos tipos penales no especifican el medio.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Según el artículo 211 bis 13 de la iniciativa, cuando la información obtenida se utilice en provecho propio o ajeno, o la realice un servidor público.

Elemento subjetivo

ELEMENTO SUBJETIVO	» Atiende al estado de conciencia, voluntad o afectividad de la persona activa. Estos tipos penales deben ser dolosos; es decir, la persona activa debe actuar teniendo conocimiento y voluntad de llevar a cabo las conductas determinadas. » *Términos vagos y amplios.* Las expresiones "acceder de manera ilegítima", "sin derecho" y "sin autorización" son abstractas. » No incluye un elemento de intencionalidad; es decir, no especifican si la persona tenía conocimiento o intención de cometer el delito. Esta *ausencia de elemento subjetivo* puede criminalizar conductas legales o conductas cometidas por error. » *Obstaculización de persecución de delitos.* El lenguaje de los tipos penales es tan similar que podrían ser el mismo delito. » Estas redacciones amplias afectan el derecho de acceso a la información y criminalizan la labor de investigadoras de seguridad informática.

DELITOS CONTRA LAS PERSONAS USUARIAS

Elemento normativo

Artículo 211 bis 7.
Artículo 211 bis 4.
Artículo 211 bis 5.

Elementos objetivos o descriptivos

CONDUCTA	» *Artículo 211 bis 7.* Adquirir información personal y financiera. » *Artículo 211 bis 4.* Obtener datos o información. » *Artículo 211 bis 5.* Copiar, modificar, limitar el acceso, corromper o destruir datos o información.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Confidencialidad, integridad y disponibilidad de la información de personas físicas y morales.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	No lo especifica.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» Estos tipos penales no especifican el medio.

CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN

» *Agravante.* Según el artículo 211 bis 13 de la iniciativa, cuando la información obtenida se utilice en provecho propio o ajeno, o la realice un servidor público.

Elemento subjetivo

ELEMENTO SUBJETIVO

» El artículo 211 bis 7 es un tipo penal doloso.

» *Términos vagos y amplios.* Las expresiones "sin autorización" y "sin autorización ni derecho" contenidas en los artículos 211 bis 4 y 5 son abstractas y no especifican si la persona tenía conocimiento o intención de cometer el delito. Esta *ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

» *Obstaculización de persecución de delitos.* El lenguaje de los tipos penales es tan similar que podrían ser el mismo delito.

» Estas redacciones amplias afectan el derecho de acceso a la información y criminalizan la labor de periodistas e investigadoras de seguridad informática.

DELITOS CONTRA EL ESTADO

Elemento normativo

Artículo 211 bis 8.
Artículo 211 bis 9.

Elementos objetivos o descriptivos

CONDUCTA	» *Artículo 211 bis 8.* Modificar, destruir, provocar pérdida de información del Estado. Conocer, copiar, obtener, utilizar información del Estado. » *Artículo 211 bis 9.* Acceder, modificar, destruir, provocar pérdida de información del Estado. Obtener, copiar, utilizar información del Estado.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	Información contenida en sistemas del Estado.
PERSONA ACTIVA	Sólo especifica el sujeto activo en caso de agravante, en cuyo caso serán los servidores públicos.
PERSONA PASIVA	El Estado.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» Estos tipos penales no especifican el medio.

CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN

» *Agravante.* Según el artículo 211 bis 13 de la iniciativa, cuando la información obtenida se utilice en provecho propio o ajeno, o la realice un servidor público. También cuando se afecte la procuración e impartición de justicia.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Términos vagos y amplios.* Las expresiones "sin autorización" y "estando autorizado pero indebidamente [realice la conducta]" son abstractas y no especifican si la persona tenía conocimiento o intención de cometer el delito. Esta *ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

» Estas redacciones amplias afectan el derecho de acceso a la información y criminalizan la labor de periodistas e investigadoras de seguridad informática. Incluso, criminalizan cualquier acceso a información realizado por un servidor público en el ejercicio de sus funciones.

DELITOS CONTRA EL SISTEMA FINANCIERO

Elemento normativo

Artículo 211 bis 10.
Artículo 211 bis 11.

Elementos objetivos o descriptivos

CONDUCTA	» *Artículo 211 bis 10.* Modificar, destruir o provocar pérdida de información del sistema financiero. Conocer o copiar información del sistema financiero. » *Artículo 211 bis 11.* Modificar, destruir copiar o provocar pérdida de información del sistema financiero.
TIPO DE RESULTADO	Resultado material.
BIEN JURÍDICO TUTELADO	El debido funcionamiento del sistema financiero mexicano.
PERSONA ACTIVA	No lo especifica.
PERSONA PASIVA	Instituciones del sistema financiero.
MEDIOS UTILIZADOS PARA REALIZAR LOS DELITOS	» Estos tipos penales no especifican el medio.
CIRCUNSTANCIAS DE LUGAR, TIEMPO, MODO U OCASIÓN	» *Agravante.* Cuando el delito lo comentan funcionarios o empleados de instituciones financieras.

Elemento subjetivo

ELEMENTO SUBJETIVO

» *Términos vagos y amplios.* Las expresiones "sin autorización" y "estando autorizado pero indebidamente [realice la conducta]" son abstractas y no especifican si la persona tenía conocimiento o intención de cometer el delito. Esta *ausencia de elemento subjetivo* criminaliza conductas legales o conductas cometidas por error.

» Estas redacciones amplias criminalizan cualquier acceso a información realizado por un empleado de instituciones financieras en el ejercicio de sus funciones.

R3D

Red en Defensa de los Derechos Digitales es una organización de la sociedad civil que se dedica a la promoción y protección de los derechos humanos en el entorno digital. A través del uso e implementación de diversas herramientas legales y de comunicación, realiza investigación, litigio estratégico, incidencia pública y campañas con el objetivo de promover y proteger los derechos digitales en México; particularmente, los derechos a la libertad de expresión, la privacidad y la protección de datos personales.

R3D
Red en Defensa
de los Derechos Digitales