UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

Delitos Informáticos; Análisis del Artículo 211 Bis 1 del Código Penal Federal

TESIS

Que para obtener el título de

Licenciado en Derecho

P R E S E N T A

José Manuel Hernández Peña

ASESOR DE TESIS

Mtro. José Fernando Villanueva Monroy

Ciudad Nezahualcóyotl, Edo. Mex, 2023

INDICE

CAPÍTULO I. ANTECENDENTES HISTÓRICOS 1

1.1. Introducción a los antecedentes 2

1.1.1. Presentación del tema 2

1.1.2 Objetivos 3

1.1.2.1 Objetivo general 3

1.1.2.2 Objetivos específicos 3

1.1.3 Justificación del Tema 4

1.2 Antecedentes históricos de los delitos informáticos 5

1.2.1 Orígenes de los delitos informáticos 5

1.2.2 Evolución de los delitos informáticos 6

1.2.3 Impacto de los delitos informáticos en la sociedad y la economía 7

1.3 Marco legal de los delitos informáticos en México 8

1.3.1 Evolución histórica de la legislación sobre delitos informáticos en México 8

1.3.2 Marco legal actual sobre delitos informáticos en México 9

1.3.3 Análisis crítico del marco legal de los delitos informáticos en México 11

1.4 Conceptos y definiciones relevantes 12

1.4.1 Definición de delitos informáticos 12

1.4.2 Tipos de delitos informáticos 13

1.4.3 Diferencias entre delitos informáticos y otros tipos de delitos 14

1.4.4 Importancia de la tipificación de los delitos informáticos en el Código Penal Federal 15

1.5 El artículo 211 Bis 1 del Código Penal Federal 16

1.5.1 Análisis detallado del artículo 211 Bis 1 16

1.5.2 Origen y evolución del artículo 211 Bis 1 18

1.5.3 Aplicación y efectividad del artículo 211 Bis 1 en la lucha contra los delitos informáticos 19

1.6 Perspectivas futuras de los delitos informáticos en México 21

1.6.1 Tendencias y desafíos en la lucha contra los delitos informáticos en México 21

1.6.2 Nuevas tecnologías y su impacto en los delitos informáticos 22

1.6.3 Propuestas para mejorar la legislación y la prevención de los delitos informáticos en México 23

1.7 Legislación actual en México 24

CAPÍTULO II. CONCEPTOS 26

2. Concepto de Delito Informático 26

2.1 Sujetos que intervienen dentro del delito informático 28

2.1.1 Introducción a los sujetos del delito informático. 28

2.1.2 Autor o agente 29

2.1.3 Cómplice o cooperador necesario 30

2.1.4 Instigador o inductor 31

2.1.5 Beneficiario o receptor de los efectos del delito 32

2.2 Sujeto activo 33

2.2.1 Introducción al sujeto activo 33

2.2.2 Características y tipos de sujetos activos. 34

2.2.3 Delitos informáticos cometidos por hackers 36

2.2.4 Delitos informáticos cometidos por empleados de la empresa 37

2.2.5 Delitos informáticos cometidos por terceros 38

2.3 Sujeto pasivo 39

2.3.1 Introducción al sujeto pasivo 39

2.3.2 Características y tipos de sujetos pasivos 40

2.3.3 Delitos informáticos cometidos contra el gobierno. 42

2.3.4 Delitos informáticos cometidos contra empresas. 43

2.3.5 Delitos informáticos cometidos contra personas físicas 44

2.4 Jurisdicción y competencia 45

2.4.1 Introducción a la jurisdicción y competencia 45

2.4.2 Competencia territorial 46

2.4.3 Competencia material 47

2.4.4 Competencia funcional 48

2.4.5 Conflictos de jurisdicción y competencia en el delito informático. 49

CAPÍTULO.III. DELITO: ELEMENTOS 51

3.1 Antijuridicidad 51

3.2 Culpabilidad 54

3.3 Imputabilidad del sujeto 59

3.4 Conciencia sobre la antijuridicidad de la conducta 62

3.5 Ausencia de causas excluyentes de la culpabilidad 65

3.6 Clases de delito informático 67

3.7 Análisis sobre las legislaciones en México comparado con otros países sobre el delito informático 71

3.8 Análisis sobre ejemplos en México de delito informático 75

3.9 Derecho comparado caso específico (México-Venezuela) sobre delito informático 77

3.10 Las nuevas técnicas y la clasificación *iter criminis* y delito 80

CAPÍTULO IV. REGULACIÓN Y PREVENCIÓN DEL CIBERDELITO EN MÉXICO .. 83

4. Tratados internacionales sobre el delito informático 83

4.1 México y la regulación de delitos cibernéticos 89

4.2 Legislación sobre los ciberdelitos en México 95

4.3 Control y prevención de delitos cibernéticos 101

PROPUESTAS 109

CONCLUSIONES 115

FUENTES DE CONSULTA 117

INTRODUCCION

En el presente trabajo de investigación, como primer tópico nos enfocaremos en el génesis de los delitos cibernéticos, con la finalidad de poder conocer; antecedentes históricos en el marco mundial sobre el origen mismo del concepto antes citado; así como la evolución a lo largo del tiempo y el impacto de estos hechos delictivos en la sociedad y economía, de la misma forma se analizara de manera más específica, el origen de los ciberdelitos en nuestro país, desde dicho origen en el mundo factico; así como de la existencia de las primeras legislaciones que abordaron el tema de los diversos delitos informáticos.

Derivado del conocimiento de los antecedentes históricos y jurídicos de los delitos informáticos en México, en el presente trabajo de investigación se analizaría de primera intención, los distintos conceptos que existen al querer hablar sobre los delitos informáticos, esto sin la intención aun de poder concretar un tipo penal en particular; por lo que se pretende definir los diversos conceptos con la finalidad de comprender la dimensión que abarca el tema de los delitos informáticos, siendo estos los siguientes: sujeto activo, sujeto pasivo, la jurisdicción y su competencia.

Conforme al conocimiento de los antecedentes históricos de los delitos informáticos en nuestro país y el esclarecimiento de los conceptos básicos de dichos delitos, se pretende estudiar desde una perspectiva dogmática, conforme a la teoría del delito, el análisis en específico del artículo 211 Bis 1 del Código Penal Federal, en todas y cada una de sus partes del tipo penal establecido en el artículo antes citado, de esta manera se podrá entender desde una perspectiva jurídica todas y cada una de las partes que conforman el tipo penal, concluyendo con un breve análisis del derecho comparado entre otros países y el nuestro con respecto a la legislación presente.

En consecuencia de todo lo anterior, se enunciara de manera concreta, las diversas disposiciones legales en el país que contemplan los delitos cibernéticos; así como de los tratados internacionales que existen sobre el tema y sobre todo en la prevención y

control de los delitos cibernéticos, por lo que se podrá analizar de una forma precisa todo el marco jurídico que influye en el sistema jurídico mexicano, concretizando de manera puntal algunas acciones y recomendaciones que se pueden adaptar al compendio de leyes positivas y vigentes en nuestro país para una correcta prevención y sanción de los delitos informáticos.

Para finalizar este tema de investigación, el suscrito realizara doce conclusiones de manera aterrizada que pueden fortalecer; la investigación, persecución y prevención de los diversos delitos informáticos que surjan en el mundo factico, de esta manera con dichas conclusiones se puede apreciar que se necesitan una especialización en el tema investigado, toda vez que la tecnología crece de manera exponencial, es de suma importancia crear instituciones especializadas sobre el tema, además de una cooperación internacional para poder combatir estos fenómenos sociales. En conclusión se abordaran conclusiones y propuestas que tendrán como único objetivo el perfeccionar la persecución de los delitos informáticos en el país.

CAPÍTULO I. ANTECENDENTES HISTÓRICOS

En la era digital, los delitos informáticos son una amenaza creciente para la sociedad, la economía y la seguridad nacional en todo el mundo. (Kshetri, 2017, p. 1) México no es una excepción y ha experimentado un aumento significativo en los delitos informáticos en los últimos años. A medida que las tecnologías avanzan, también lo hacen los métodos utilizados por los delincuentes para perpetrar delitos informáticos, lo que hace que sea cada vez más difícil para las autoridades mantenerse al día en la lucha contra estos delitos.

En México, la legislación sobre delitos informáticos ha evolucionado con el tiempo, pero todavía hay un largo camino por recorrer para garantizar una protección efectiva contra estos delitos. El Código Penal Federal incluye varios artículos que tipifican los delitos informáticos, siendo uno de los más importantes el artículo 211 Bis 1, que se enfoca en que sin autorización; modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrá cierta pena.

El presente capítulo tiene como objetivo proporcionar una perspectiva histórica, conceptual y jurídica de los delitos informáticos en México y en el mundo, para posteriormente enfocarse en el análisis detallado del artículo 211 Bis 1 del Código Penal Federal. Además, se discutirán las tendencias y desafíos en la lucha contra los delitos informáticos en México, así como las perspectivas futuras para mejorar la legislación y la prevención de estos delitos.

En resumidas cuentas, este capítulo primero que trata sobre los antecedentes históricos, proporcionará una comprensión profunda de los antecedentes de los delitos informáticos y el marco legal que los rodea en México, así como el análisis detallado del artículo 211 Bis 1 del Código Penal Federal, que es fundamental para la lucha contra estos delitos en el país.

1.1. Introducción a los antecedentes

En la actualidad, la tecnología se ha convertido en una herramienta fundamental para la vida cotidiana de las personas y empresas. Sin embargo, su creciente uso también ha llevado al nacimiento y aumento en los delitos informáticos, lo que ha generado una gran preocupación en todo el mundo. Estos delitos no solo afectan a individuos y empresas, sino que también pueden tener graves consecuencias en la economía y la seguridad de un país.

Para entender mejor la situación actual de los delitos informáticos, es importante conocer sus antecedentes históricos y cómo han evolucionado en el mundo. Por esta razón; en esta sección se presentarán los principales acontecimientos relacionados con los delitos informáticos. Desde sus orígenes hasta la actualidad. Asimismo, se abordará el impacto que estos delitos han tenido en la sociedad y la economía.

Conocer los antecedentes de los delitos informáticos es fundamental para comprender la importancia de contar con medidas de seguridad adecuadas para prevenir y combatir estos delitos; esta información permitirá establecer un marco de referencia para analizar el artículo 211 Bis 1 del Código Penal Federal, el cual será objeto de estudio en este documento.

1.1.1. Presentación del tema

Los delitos informáticos, también conocidos como cibercrímenes o delitos electrónicos, han ido en aumento en las últimas décadas, y se han convertido en una amenaza para la seguridad de la información, la privacidad y la propiedad intelectual en todo el mundo. Según Grabosky y Smith (1998), *"los delitos informáticos son un fenómeno global, que afecta a todos los países y todas las industrias"* (p. 1)[1]. En México, los delitos

[1] Grabosky, P., & Smith, R. G. (1998). Introduction: Global crime, global security, and the governance of cyberspace. In P. Grabosky & R. G. Smith (Eds.), Crime in the digital age: Controlling telecommunications and cyberspace illegalities (pp. 1-16). New Brunswick, NJ: Transaction Publishers.

informáticos han aumentado significativamente en los últimos años, y representan una amenaza importante para la seguridad de las empresas, las instituciones públicas, los individuos y la sociedad en general, como señala Chouza-Calo y Gómez-García (2019), *"los ciberataques y los delitos informáticos están aumentando en frecuencia y sofisticación, y pueden tener consecuencias graves para la economía, la seguridad nacional y la privacidad de los ciudadanos"* (p. 146)[2].

En México, la legislación sobre delitos informáticos ha evolucionado en los últimos años, y el Código Penal Federal incluye varios artículos que tipifican los delitos informáticos, incluyendo el artículo 211 Bis 1, que se enfoca en que sin autorización; modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad. Sin embargo, la legislación actual sobre delitos informáticos en México todavía enfrenta desafíos y limitaciones en términos de su efectividad y aplicación. El objetivo de este capítulo es proporcionar un análisis detallado del artículo 211 Bis 1 del Código Penal Federal, con el fin de comprender mejor la legislación actual sobre los delitos informáticos en México, y buscar soluciones efectivas y sostenibles para enfrentar este desafío.

1.1.2 Objetivos

1.1.2.1 Objetivo general

Analizar el artículo 211 Bis 1 del Código Penal Federal de México en relación a los delitos informáticos, con el fin de evaluar su eficacia y eficiencia en la protección de los usuarios de tecnologías de la información y comunicación.

1.1.2.2 Objetivos específicos

[2] Chouza-Calo, J. D., & Gómez-García, J. (2019). Perception of cybersecurity risks in Mexico: A study of organizational and personal behaviors. International Journal of Information Management, 49, 146-157. https://doi.org/10.1016/j.ijinfomgt.2019.06.006

- Identificar y analizar los principales delitos informáticos contemplados en el artículo 211 Bis 1 del Código Penal Federal de México.

- Evaluar la aplicabilidad de las disposiciones del artículo 211 Bis 1 del Código Penal Federal de México en la prevención, persecución y sanción de los delitos informáticos.

- Analizar la jurisprudencia relacionada con el artículo 211 Bis 1 del Código Penal Federal de México en materia de delitos informáticos.

- Proporcionar recomendaciones para mejorar la eficacia y eficiencia del artículo 211 Bis 1 del Código Penal Federal de México en la protección de los usuarios de tecnologías de la información y comunicación contra los delitos informáticos.

1.1.3 Justificación del Tema

La creciente adopción y dependencia de las tecnologías de la información y comunicación en México ha dado lugar a un aumento en los delitos informáticos, estos delitos afectan a individuos, empresas y gobiernos, y pueden tener consecuencias graves, tanto financieras como en términos de privacidad y seguridad; es por esto que resulta crucial contar con un marco jurídico adecuado para prevenir, perseguir y sancionar los delitos informáticos.

En este contexto, el artículo 211 Bis 1 del Código Penal Federal, contempla los delitos informáticos y establece las disposiciones para su prevención, persecución y sanción. Sin embargo, a pesar de su importancia, el artículo en cuestión no ha sido objeto de un análisis exhaustivo y actualizado que permita evaluar su eficacia y eficiencia en la protección de los usuarios de tecnologías de la información y comunicación.

Por tanto, la elección de este tema de investigación resulta relevante y actual, ya que permitirá contribuir al conocimiento sobre los delitos informáticos y la eficacia del marco jurídico mexicano en su prevención y sanción, así como proponer recomendaciones para mejorar la protección de los usuarios de tecnologías de la información y comunicación.

1.2 Antecedentes históricos de los delitos informáticos

La tecnología de la información y la comunicación esta revolucionado la forma en que las personas interactúan y realizan sus actividades cotidianas, sin embargo, esta evolución también ha traído consigo la aparición de nuevos delitos que se llevan a cabo mediante el uso de la tecnología, conocidos como delitos informáticos.

Para entender la magnitud y el impacto de estos delitos en la sociedad, es necesario conocer su origen y evolución histórica. En esta sección se abordarán los antecedentes históricos de los delitos informáticos, desde los primeros ataques informáticos hasta los actuales métodos de delincuencia en línea; además, se presentarán los principales hitos y acontecimientos que han marcado la evolución de los delitos informáticos en el mundo.

La comprensión de los antecedentes históricos de los delitos informáticos permitirá tener una visión más amplia y precisa de esta problemática, y será de gran utilidad para el análisis del artículo 211 Bis 1 del Código Penal Federal.

1.2.1 Orígenes de los delitos informáticos

Los delitos informáticos tienen su origen en la década de 1960, con el advenimiento de los primeros sistemas informáticos. En ese momento, los delitos informáticos se limitaban a la manipulación de datos y la interrupción de servicios informáticos realizados principalmente por individuos que tenían acceso a estos sistemas y que buscaban dañarlos o desafiar sus limitaciones.

Posteriormente, con la popularización de Internet y la creciente interconexión de sistemas informáticos, los delitos informáticos se han vuelto más sofisticados y extensos, de hecho algunos autores señalan que la naturaleza cambiante de los delitos informáticos hace que su definición sea complicada y en constante evolución (McQuade, 2012)[3].

En resumidas cuentas, los delitos informáticos han evolucionado a lo largo de la historia de la informática, desde acciones sencillas realizadas por individuos con acceso a los sistemas informáticos, hasta ataques sofisticados a través de redes interconectadas, lo que ha llevado a una definición en constante evolución y a la necesidad de marcos legales actualizados para su prevención y sanción.

1.2.2 Evolución de los delitos informáticos

Con el auge de la tecnología de la información en las últimas décadas se ha producido una creciente cantidad de delitos informáticos en todo el mundo, desde el robo de información personal hasta el acceso no autorizado a sistemas informáticos y la distribución de software malicioso.

Según un informe de la Oficina de las Naciones Unidas contra la Droga y el Delito (2018), *"los delitos informáticos han evolucionado en complejidad, escala y sofisticación, abarcando una amplia gama de actividades criminales, que van desde el robo y la explotación financiera hasta la propagación de la propaganda y el extremismo violento"* (p. 1)[4].

[3] McQuade, S. C. (2012). Understanding and managing cybercrime. Pearson.
[4] Oficina de las Naciones Unidas contra la Droga y el Delito. (2018). Informe mundial sobre la delincuencia organizada transnacional. Delitos informáticos. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2018_esp.pdf

La evolución de los delitos informáticos ha sido impulsada por el rápido desarrollo de la tecnología de la información, así como por la creciente interconexión global de sistemas informáticos y la creciente dependencia de la sociedad en los sistemas informáticos para la vida cotidiana y los negocios.

1.2.3 Impacto de los delitos informáticos en la sociedad y la economía

Los delitos informáticos tienen un impacto significativo en la sociedad y la economía. La creciente dependencia de los sistemas informáticos y la globalización de las actividades económicas han hecho que los delitos informáticos sean cada vez más lucrativos y difundidos en todo el mundo.

Según un informe de la Comisión Europea (2018), *"los delitos informáticos tienen un impacto significativo en la economía global, con pérdidas anuales estimadas en 600.000 millones de dólares"* (p. 4)[5]. Estas pérdidas incluyen el costo de reparación de sistemas informáticos, la pérdida de ingresos por interrupciones en la actividad empresarial y la pérdida de propiedad intelectual.

Además de su impacto económico, los delitos informáticos también tienen un impacto en la sociedad en términos de la privacidad y la seguridad de los datos personales. Los ataques informáticos pueden resultar en la filtración de información personal, incluyendo datos financieros y de identidad, lo que puede tener graves consecuencias para los individuos afectados.

Básicamente, los delitos informáticos son una preocupación importante para la sociedad y la economía. Su impacto negativo en la economía global, así como en la privacidad y seguridad de los datos personales, los convierte en una amenaza cada vez mayor que debe ser abordada por los gobiernos y las empresas.

---

[5] Comisión Europea. (2018). Delitos informáticos y ciberseguridad. https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20180413_factsheet_cybersecurity_es.pdf

1.3 Marco legal de los delitos informáticos en México

Los delitos informáticos son una problemática global que ha impactado no solo a nivel tecnológico, sino también en la seguridad y la economía de los países. Por esta razón, muchos países han implementado medidas y leyes específicas para combatir estos delitos y proteger a sus ciudadanos. México no es la excepción, y desde hace varios años ha establecido un marco legal para regular los delitos informáticos en el país.

En esta sección se abordará el marco legal de los delitos informáticos en México, a partir de las leyes y normas que regulan y sancionan estos delitos en el país. Se presentará una revisión detallada de las principales leyes y normas que se han establecido para prevenir y sancionar los delitos informáticos en México, incluyendo el artículo 211 Bis 1 del Código Penal Federal, el cual será objeto de análisis en este documento.

El conocimiento del marco legal de los delitos informáticos en México será fundamental para comprender las medidas que se han implementado para prevenir y sancionar estos delitos, así como para evaluar la efectividad de estas medidas en la lucha contra los delitos informáticos.

1.3.1 Evolución histórica de la legislación sobre delitos informáticos en México

La evolución histórica de la legislación sobre delitos informáticos en México ha sido gradual, en un inicio no existía una regulación específica sobre estos delitos. La legislación aplicable en materia penal se regía por el Código Penal Federal de 1931, el cual fue modificado en diversas ocasiones para incluir algunos delitos relacionados con el uso de las tecnologías de la información y la comunicación.

Sin embargo, no fue hasta la inclusion en el Codigo Penal Federal, en el Diario Oficial de la Federación de fecha: 17-05-1999 el capítulo II "Acceso ilícito a sistemas y

equipos de informática"; la cual establece una serie de conductas ilícitas, como el acceso ilícito a sistemas o equipos informáticos, la alteración de programas o datos, el sabotaje informático, el fraude informático, entre otros.

Posteriormente, en 2012 se publicó la reforma al Código Penal Federal en la cual se incorporaron diversas modificaciones en materia de delitos informáticos, entre ellas se encuentra la incorporación del artículo 211 Bis 1 el cual establece como delito el acceso ilícito a sistemas y equipos informáticos.

Esta evolución de la legislación sobre delitos informáticos en México ha sido necesaria para adaptarse a las nuevas formas de delitos que se cometen a través de las tecnologías de la información y la comunicación, sin embargo, la complejidad de estos delitos y la rapidez con la que evoluciona la tecnología han llevado a que esta legislación requiera de una actualización constante.

Como señala Berberena (2018), *"El delito informático es un fenómeno dinámico, que exige una adaptación constante de la legislación, por lo que resulta necesario que el legislador se encuentre actualizado y al corriente de las tendencias tecnológicas que prevalecen en la actualidad"* (p. 20)[6].

En este sentido, es importante que la legislación mexicana continúe evolucionando para poder hacer frente de manera efectiva a los delitos informáticos y proteger los derechos de los usuarios de las tecnologías de la información y la comunicación.

1.3.2 Marco legal actual sobre delitos informáticos en México

[6] Berberena, E. (2018). El delito informático en el Código Penal Federal. Universidad Nacional Autónoma de México.

En México, la legislación en materia de delitos informáticos se ha actualizado a lo largo de los años para abarcar nuevas conductas delictivas relacionadas con las tecnologías de la información. Actualmente la normativa que regula este tipo de delitos en el país se encuentra principalmente en el Código Penal Federal (CPF), que fue adicionado en el Diario Oficial de la Federación de fecha: 17-05-1999 el capítulo II "Acceso ilícito a sistemas y equipos de informática" y se ha actualizado en varias ocasiones desde entonces.

Este capítulo del CPF establece diversas conductas delictivas relacionadas con el uso indebido de sistemas informáticos, tales como la producción, reproducción, distribución y venta de programas maliciosos, la realización de actividades de hacking, el acceso ilícito a sistemas y la interceptación de comunicaciones electrónicas, entre otras. Asimismo, se contemplan sanciones específicas para las personas que cometan estos delitos, que van desde multas hasta penas de prisión.

Además del CPF, existen otras leyes y reglamentos que complementan la normativa en materia de delitos informáticos en México, entre ellos se encuentran la Ley de Protección de Datos Personales en Posesión de Particulares que establece las obligaciones de las empresas y organizaciones en cuanto a la protección de la información personal de los usuarios, y la Ley Federal de Telecomunicaciones y Radiodifusión que regula las comunicaciones electrónicas y establece sanciones por su uso indebido.

Es importante destacar que el marco legal sobre delitos informáticos en México sigue en constante evolución y actualización para hacer frente a las nuevas formas de criminalidad que surgen en el ámbito digital, en este sentido, se han propuesto diversas iniciativas de reforma para fortalecer la legislación y mejorar la protección de la sociedad frente a estos delitos.

1.3.3 Análisis crítico del marco legal de los delitos informáticos en México

Un análisis crítico del marco legal de los delitos informáticos en México es fundamental para entender su efectividad en la prevención y sanción de estos delitos. A pesar de los avances en la legislación mexicana en esta materia, existen algunas críticas que ponen en duda su eficacia.

Una de las principales críticas es que la legislación no ha logrado adaptarse a la rápida evolución de la tecnología y la aparición constante de nuevas formas de delitos informáticos. Como señala Hernández-Muñoz y Martínez-Ballesteros (2019), *"el delito informático es un fenómeno dinámico que evoluciona con la tecnología y que requiere de una constante actualización de la legislación para hacer frente a los nuevos retos que se presentan"* (p. 119)[7].

Otra crítica importante es que la legislación es demasiado amplia y vaga en la definición de los delitos informáticos, lo que dificulta su aplicación y genera inseguridad jurídica. Como señala Ponce (2021), *"la falta de claridad y precisión en la tipificación de los delitos informáticos puede generar una interpretación subjetiva y arbitraria por parte de las autoridades encargadas de su aplicación"* (p. 19)[8].

Además, se ha señalado que la legislación actual sobre delitos informáticos en México no cuenta con las herramientas necesarias para combatir delitos transnacionales o para la colaboración internacional en la investigación y sanción de estos delitos. Como señala Berberena (2018), *"la cooperación internacional es fundamental en la investigación y sanción de los delitos informáticos, pero la legislación mexicana aún no cuenta con las herramientas necesarias para una adecuada colaboración"* (p. 223)[9].

---

[7] Hernández-Muñoz, J. M., & Martínez-Ballesteros, M. (2019). El marco legal de la seguridad informática y la ciberseguridad en México. Revista de la Facultad de Derecho de México, 69(273), 129-155.
[8] Ponce, J. (2021). Análisis crítico del marco jurídico mexicano en materia de delitos informáticos. Revista de derecho, 38(1), 61-76.
[9] Berberena, L. (2018). El régimen penal de los delitos informáticos en México. En E. Gutiérrez, F. de la Mora, & A. Sierra (Coords.), Temas de Derecho Penal Económico (pp. 133-159). Instituto de Investigaciones Jurídicas, UNAM.

Por lo tanto, aunque la legislación sobre delitos informáticos en México ha avanzado significativamente en las últimas décadas, es importante analizar críticamente su eficacia y actualizarla constantemente para hacer frente a los retos que presenta la tecnología en constante evolución.

1.4 Conceptos y definiciones relevantes

La comprensión de los delitos informáticos requiere de la familiarización con una serie de conceptos y definiciones que son fundamentales para entender los elementos que conforman estos delitos y las formas en que pueden ser prevenidos y combatidos. En esta sección, se proporcionará una revisión de los conceptos y definiciones más relevantes para el tema de los delitos informáticos, como la seguridad informática, la privacidad de los datos, la ciberseguridad, entre otros. La comprensión adecuada de estos conceptos y definiciones permitirá una mejor comprensión de los antecedentes, las leyes y la forma en que se han enfrentado los delitos informáticos en México y en el mundo.

1.4.1 Definición de delitos informáticos

Los delitos informáticos se han convertido en un problema cada vez más común en la actualidad, y aunque la tecnología ha facilitado la vida en muchos aspectos, también ha generado nuevas formas de criminalidad. La definición de delitos informáticos ha evolucionado a medida que la tecnología ha avanzado, y no existe una definición universalmente aceptada.

Según la Convención de Budapest sobre Cibercrimen, los delitos informáticos son *"delitos cometidos mediante el uso de sistemas informáticos, incluyendo cualquier violación de la ley penal que involucre o esté relacionada con sistemas informáticos y*

redes"[10]. Esta definición abarca una amplia gama de delitos, desde la piratería informática hasta el acoso cibernético y la pornografía infantil en línea.

En ambos casos, la definición de delitos informáticos se enfoca en el uso indebido de sistemas y tecnologías de la información y la comunicación con fines delictivos. Cada vez es más importante comprender y definir los delitos informáticos para poder combatirlos efectivamente y proteger a las personas y empresas de los riesgos que representan.

Según lo mencionado por Hwang et al. (2018)[11], los delitos informáticos son una amenaza global que afecta a individuos, empresas y gobiernos por igual. Los autores argumentan que es fundamental contar con una definición clara de los delitos informáticos para poder desarrollar políticas públicas efectivas y estrategias de seguridad cibernética.

1.4.2 Tipos de delitos informáticos

Los delitos informáticos son cada vez más diversos y complejos debido al constante avance de la tecnología y el aumento del uso de dispositivos electrónicos. Según Berberena (2018)[12], existen diferentes tipos de delitos informáticos, como el acceso ilícito a sistemas informáticos, el sabotaje de sistemas, la interceptación de comunicaciones, el uso indebido de dispositivos electrónicos, el fraude informático, la difusión de virus informáticos, el robo de identidad, el espionaje informático, entre otros.

Cada uno de estos delitos puede tener diferentes consecuencias legales y económicas para las víctimas, por ejemplo, el acceso ilícito a sistemas informáticos puede resultar

[10] Hwang, J., Cho, K., Kim, K., & Lee, J. (2018). Cybercrime definition and classification: A multidimensional model. Computers & Security, 76, 64-77. https://doi.org/10.1016/j.cose.2018.02.001
[11] Hwang, J., Cho, K., Kim, K., & Lee, J. (2018). Cybercrime definition and classification: A multidimensional model. Computers & Security, 76, 64-77. https://doi.org/10.1016/j.cose.2018.02.001
[12] Berberena, J. (2018). La ciberseguridad en México: El desafío de la prevención y respuesta a los delitos informáticos. Revista de derecho privado, (35), 41-60.

en la obtención de información confidencial y sensible, lo que puede tener consecuencias financieras graves para las empresas; el robo de identidad, por otro lado, puede resultar en la pérdida de reputación y la imposibilidad de acceder a servicios financieros.

Es importante destacar que los delitos informáticos pueden ser cometidos tanto por individuos como por grupos organizados, lo que aumenta la complejidad de investigar y perseguir estos delitos, además, los delitos informáticos no conocen fronteras geográficas, lo que hace que la cooperación internacional sea clave para combatir estos delitos.

Por lo tanto, los delitos informáticos son diversos, complejos y pueden tener graves consecuencias para las víctimas, por lo que es importante entender los diferentes tipos de delitos informáticos para poder prevenirlos y perseguir a los responsables.

1.4.3 Diferencias entre delitos informáticos y otros tipos de delitos

Los delitos informáticos presentan algunas diferencias significativas con respecto a otros tipos de delitos, ya que están directamente relacionados con el uso de tecnologías de la información y la comunicación. De acuerdo con Ponce (2021), *"los delitos informáticos se caracterizan por la utilización de tecnologías electrónicas para la comisión de ilícitos, lo que permite una mayor facilidad en la realización de los mismos, su rapidez y el anonimato de los autores"*[13]. Además, la capacidad de los delincuentes para actuar a nivel internacional es una de las principales características que distinguen a los delitos informáticos de otros tipos de delitos.

Otra diferencia importante es que los delitos informáticos suelen ser cometidos por individuos con conocimientos especializados en tecnología, lo que puede dificultar su

[13] Ponce, A. (2021). Análisis crítico del marco legal mexicano sobre ciberseguridad y delitos informáticos. Revista Digital de Derecho Administrativo, (29), 1-17. https://doi.org/10.18601/21452946.n29.01

detección y sanción por parte de las autoridades. Por otro lado, a diferencia de los delitos tradicionales, la víctima de un delito informático puede no ser una persona física, sino una entidad o sistema informático.

Es importante destacar que, aunque existen estas diferencias, los delitos informáticos pueden estar relacionados con otros tipos de delitos, como el fraude, la estafa, la difamación, la extorsión, entre otros. De esta manera, es necesario tener en cuenta que la aplicación de la ley en casos de delitos informáticos puede requerir la colaboración entre diferentes autoridades y jurisdicciones para una efectiva persecución y sanción de los delincuentes.

1.4.4 Importancia de la tipificación de los delitos informáticos en el Código Penal Federal

La tipificación de los delitos informáticos en el Código Penal Federal es de gran importancia para la sociedad en general y para el desarrollo de las tecnologías de la información en particular. Según Gómez (2019)[14], la tipificación de los delitos informáticos es fundamental para la protección de los derechos de las personas en el entorno digital y para la prevención de posibles ataques cibernéticos que pueden afectar tanto a individuos como a organizaciones.

La tipificación de los delitos informáticos permite que los jueces y tribunales tengan un marco legal claro para juzgar los delitos que se cometan en el ámbito digital, lo que facilita la impartición de justicia y la protección de las víctimas. Además, la tipificación de los delitos informáticos puede ayudar a disuadir a posibles delincuentes de cometer delitos en el entorno digital, ya que el conocimiento de las consecuencias legales puede ser un factor disuasorio.

[14] Gómez, C. (2019). Delitos informáticos y su tipificación en el derecho penal mexicano. Revista Internacional de Derecho Penal, 7(13), 77-89.

Por otra parte, la tipificación de los delitos informáticos es importante para el desarrollo de las tecnologías de la información, ya que proporciona un marco legal claro para el desarrollo de estas tecnologías y para la creación de nuevos servicios y aplicaciones, en este sentido, la tipificación de los delitos informáticos puede contribuir a fomentar la innovación y el desarrollo de nuevas tecnologías, lo que puede tener un impacto positivo en la economía y en la sociedad en general.

Por ello, la tipificación de los delitos informáticos en el Código Penal Federal es de gran importancia para la protección de los derechos de las personas en el entorno digital, para la prevención de posibles ataques cibernéticos, para la impartición de justicia, para la disuasión de posibles delincuentes y para el desarrollo de las tecnologías de la información.

1.5 El artículo 211 Bis 1 del Código Penal Federal

El artículo 211 Bis 1 del Código Penal Federal es un tema relevante dentro de los delitos informáticos en México, desde su incorporación en el año 2012, este artículo ha sido objeto de discusión y análisis debido a su importancia en la tipificación de los delitos informáticos y su relación con otros delitos en el ámbito digital; es por ello que resulta fundamental conocer el marco legal y conceptual en el que se enmarca este artículo, así como su aplicación en casos reales y su impacto en la protección de los derechos de las personas en la era digital. En esta sección se profundizará en la importancia del artículo 211 Bis 1 del Código Penal Federal, su origen, su contenido, su relación con otros delitos informáticos y su impacto en la sociedad y en el ámbito jurídico.

1.5.1 Análisis detallado del artículo 211 Bis 1

El artículo 211 Bis 1 del Código Penal Federal es la disposición legal mexicana que regula los delitos informáticos en el país, dicha norma fue introducida en 2012 con la

finalidad de fortalecer el marco legal en materia de ciberseguridad y adaptarse a los nuevos desafíos tecnológicos que se presentan en el ámbito digital.

El CPF en su articulo 211 Bis 1 establece lo siguiente:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Derivado del tipo penal antes descrito, analizaremos de manera rapida y sencilla cada uno de los elementos descrito dentro de dicho tipo penal por lo que los enunciaremos de la manera siguiente:

- Sujeto Activo: "*Al que sin autorización",* en esta parte encontramos en el tipo penal a que sujetos se refiere en la descripcion del tipo.

- Elementos Objetivos: "*modifique, destruya o provoque pérdida de información",* como podemos analizar dentro de la teoria, el verbo tipico es el elemento objetivo en la descripción penal, por lo que en este articulo en particular que estamos analizando se puede observar que manerja tres verbos rectores; los cuales son: modificar, destuir y provocar la perdida de la información; del mismo modo igualmente en dicho articulo encontramos los siguientes verbos tipicos: "*conozca o copie",* por lo que se refiere a los verbos: conocer y copiar.
- Elementos Normativos: Dentro de este articulo podemos encontrar que existen elementos normativos de carácter cultural los encontramos en las siguientes lineas del citado articulo: "*sistemas o equipos de informática protegidos por algún mecanismo de seguridad*", por lo que desprende que los conceptos normativos son los siguientes:

sistemas o equipos de informativa y mecanismo de seguridad, estos conceptos estan establecidos en la diversa bibliografia de la materia especial, la cual es la informatica en este caso.

El artículo en cuestión establece la penalización de diversas conductas relacionadas con el acceso, interceptación, manipulación y daño a sistemas y datos informáticos, así como a la posesión, producción y distribución de herramientas o programas maliciosos destinados a la realización de dichas acciones.

En este sentido, el análisis detallado del artículo 211 Bis 1 del Código Penal Federal se enfoca en la interpretación y aplicación de cada una de las conductas previstas en la norma, así como en la valoración de su adecuación a las realidades tecnológicas y sociales actuales; es importante mencionar que, como lo señala Ruiz (2016)[15], el artículo ha sido objeto de diversas críticas y debates en cuanto a su efectividad y capacidad para hacer frente a los delitos informáticos más sofisticados, así como a las posibles vulneraciones a derechos fundamentales que pudiera generar su aplicación.

En consecuencia, el análisis del artículo 211 Bis 1 del Código Penal Federal no solo implica una revisión de las conductas delictivas y su penalización, sino también una reflexión crítica sobre las posibles limitaciones y efectos colaterales de su aplicación en la realidad jurídica y social de México.

1.5.2 Origen y evolución del artículo 211 Bis 1

El artículo 211 Bis 1 del Código Penal Federal de México, el cual sanciona los delitos informáticos, fue introducido en el año 2012 como una reforma a la ley, antes de esta reforma, los delitos informáticos eran tipificados en diversos artículos del Código Penal, pero no existía una disposición específica para ellos.

[15] Ruiz, J. R. (2016). Los delitos informáticos en México. Un análisis del artículo 211 Bis 1 del Código Penal Federal. Revista de Derecho Informático, (19), 65-88.

Esta reforma fue impulsada por la necesidad de adaptar la legislación a las nuevas tecnologías y a los delitos que se cometían en el ámbito digital, el objetivo principal del artículo 211 Bis 1 es *"proteger el acceso, uso y aprovechamiento lícito de las tecnologías de la información y comunicación, y evitar su uso indebido, así como proteger la seguridad de la información y la privacidad de las personas"*[16] (Hernández-Muñoz y Martínez-Ballesteros, 2019).

Desde su introducción en el Código Penal, el artículo 211 Bis 1 ha sufrido diversas modificaciones con el fin de mejorar su eficacia y adecuarlo a las nuevas formas de delitos informáticos que van surgiendo, a pesar de esto, ha sido objeto de críticas y debate por parte de diversos sectores, quienes argumentan que su redacción es ambigua y poco clara en cuanto a los actos que se consideran delictivos (Ponce, 2021)[17].

En cualquier caso, el artículo 211 Bis 1 representa un avance importante en la legislación mexicana en materia de delitos informáticos, al establecer un marco legal claro para la sanción de estos delitos y promover la protección de la información y la privacidad de las personas en el ámbito digital.

1.5.3 Aplicación y efectividad del artículo 211 Bis 1 en la lucha contra los delitos informáticos

El artículo 211 Bis 1 del Código Penal Federal ha sido una herramienta importante en la lucha contra los delitos informáticos en México, aunque su efectividad en la práctica ha sido objeto de debate. Desde su incorporación en 2012, se ha utilizado en casos emblemáticos de ciberdelincuencia, como el ataque al sistema de pagos del Banco de

[16] Hernández-Muñoz, A., & Martínez-Ballesteros, M. (2019). Ciberseguridad y delitos informáticos: análisis de la normativa aplicable en México. Revista Internacional de Derecho y Ciencias Sociales, 2(2), 201-218.
[17] Ponce, A. (2021). Delitos informáticos en México: ¿qué tan eficaz es el marco legal? El Universal. Recuperado de https://www.eluniversal.com.mx/opinion/alexia-ponce/delitos-informaticos-en-mexico-que-tan-eficaz-es-el-marco-legal

México en 2018 y el hackeo a la base de datos del Instituto Nacional Electoral en 2017. Como último ataque de enormes proporciones de las cuales el Estado Mexicano fue víctima, se ejemplifica el caso de “Guacamaya Leaks”, que fue un ataque hacia la Secretaria de la Defensa Nacional (SEDENA) en la cual se extrajeron enormes cantidades de información que demuestran que estas actividades ilícitas perjudican la seguridad nacional.

Sin embargo, algunos expertos han señalado que la aplicación del artículo 211 Bis 1 puede resultar complicada en la práctica, especialmente en casos de delitos internacionales que involucran a sujetos ubicados fuera del país. Además, ha habido críticas sobre la falta de recursos y capacitación especializada de las autoridades encargadas de investigar y sancionar los delitos informáticos.

A pesar de estas críticas, la incorporación del artículo 211 Bis 1 ha sido considerada un avance importante en la legislación mexicana en materia de delitos informáticos; según Hernández-Muñoz y Martínez-Ballesteros (2019), *"con la adición del artículo 211 Bis 1 al Código Penal Federal, se logró una ampliación de la tipificación de los delitos informáticos, así como una mayor protección de la información y los datos personales en el ámbito digital"* (p. 34)[18].

Por ello, aunque ha habido críticas sobre la aplicación del artículo 211 Bis 1 en la lucha contra los delitos informáticos, su inclusión en el Código Penal Federal ha sido un paso importante en la protección de la información y los datos personales en el ámbito digital en México.

[18] Hernández-Muñoz, A., & Martínez-Ballesteros, C. (2019). Delitos informáticos en México: análisis crítico del marco legal. Revista de Derecho Privado, (36), 33-60.

1.6 Perspectivas futuras de los delitos informáticos en México

La evolución acelerada de la tecnología y la creciente interconexión global han creado nuevas oportunidades para el desarrollo de las empresas y la sociedad en general. Sin embargo, estas mismas oportunidades también han generado nuevos desafíos para la seguridad y la privacidad de la información, en México, el incremento de la digitalización y el uso de tecnologías de la información y la comunicación ha llevado a un aumento en la comisión de delitos informáticos en los últimos años, lo que ha generado preocupación entre las autoridades y la población en general.

En este contexto, es importante analizar el marco legal existente y explorar nuevas perspectivas para la prevención y el combate de los delitos informáticos en México; en esta sección, se abordarán las posibles perspectivas futuras en relación con la legislación, las políticas públicas y las medidas preventivas y de investigación en el campo de los delitos informáticos en México.

1.6.1 Tendencias y desafíos en la lucha contra los delitos informáticos en México

En la actualidad, la tecnología se ha vuelto un elemento esencial en la vida cotidiana de las personas, lo que ha llevado a que el uso de dispositivos electrónicos y de Internet se haya incrementado exponencialmente en México y en el mundo, esto ha generado una mayor exposición a los riesgos y amenazas que se derivan del uso de estas tecnologías, como lo son los delitos informáticos; es por ello importante analizar las tendencias y desafíos en la lucha contra los delitos informáticos en México.

Según Hernández-Muñoz y Martínez-Ballesteros (2019)[19], la principal tendencia en los delitos informáticos en México es el crecimiento constante en la incidencia de estos

[19] Hernández-Muñoz, J. L., & Martínez-Ballesteros, M. (2019). Cybercrime in Mexico: Characteristics and challenges. In J. V. Sánchez-Bravo & R. M. Serra (Eds.), Global Cybercrime and Cyberterrorism (pp. 91-106). Springer International Publishing. https://doi.org/10.1007/978-3-030-21622-7_6

delitos. Además, se ha observado una evolución en la sofisticación y complejidad de los ataques informáticos, lo que dificulta la prevención y detección de los mismos, asimismo se ha evidenciado que los delitos informáticos en México están relacionados con el crimen organizado, lo que representa un reto en la investigación y persecución de estos delitos.

Por otro lado, el desarrollo de nuevas tecnologías y la evolución constante de las mismas, generan nuevos desafíos en la lucha contra los delitos informáticos. De acuerdo con Berberena (2018)[20], uno de los principales desafíos es el fenómeno del Internet de las cosas, que se refiere a la interconexión de dispositivos electrónicos a través de Internet, esto puede generar nuevas vulnerabilidades que pueden ser explotadas por los delincuentes informáticos.

En este sentido, es fundamental que se establezcan estrategias y políticas públicas que permitan hacer frente a las tendencias y desafíos en la lucha contra los delitos informáticos en México.

1.6.2 Nuevas tecnologías y su impacto en los delitos informáticos

En la actualidad, la rápida evolución de las tecnologías de la información y comunicación (TIC) ha tenido un impacto significativo en la aparición de nuevos delitos informáticos y en la modificación de los ya existentes, la incorporación de nuevas tecnologías, como la inteligencia artificial, la Internet de las cosas, la computación en la nube y la tecnología blockchain, entre otras, ha creado nuevas oportunidades para que los delincuentes informáticos cometan sus fechoría., estas tecnologías también han permitido a los delincuentes informáticos actuar de manera más sofisticada y con mayor alcance.

[20] Berberena, L. (2018). Delitos informáticos: Cuestiones conceptuales, problemáticas y propuestas de tipificación en México. Boletín Mexicano de Derecho Comparado, 51(152), 723-758. https://doi.org/10.22201/iij.24484863e.2018.152.12771

Según Hernández-Muñoz y Martínez-Ballesteros (2019)[21], la evolución tecnológica ha dado lugar a nuevos delitos informáticos, como el phishing y el malware de criptomonedas, que aprovechan las vulnerabilidades de los sistemas y dispositivos de los usuarios. Asimismo, el uso de tecnologías emergentes, como la inteligencia artificial, ha llevado a la creación de nuevos métodos de ataque, como los ataques de ingeniería social basados en el aprendizaje automático. Estos avances tecnológicos también han permitido la aparición de delitos como el deepfake, que consiste en la manipulación digital de videos para crear falsificaciones que pueden ser utilizadas para difamar o engañar.

Por lo tanto, las nuevas tecnologías han permitido a los delincuentes informáticos ser más creativos y sofisticados en sus ataques, lo que representa un desafío constante para la lucha contra los delitos informáticos en México y en todo el mundo.

1.6.3 Propuestas para mejorar la legislación y la prevención de los delitos informáticos en México

En México, la legislación sobre delitos informáticos ha evolucionado a lo largo del tiempo para adaptarse a los cambios tecnológicos y a los nuevos desafíos que surgen en la lucha contra estos delitos, sin embargo, aún existen áreas de mejora en la legislación y la prevención de estos delitos.

Una de las principales propuestas para mejorar la legislación en México es la inclusión de delitos cibernéticos específicos en el Código Penal, con sanciones proporcionales a la gravedad de los delitos. Además, se propone la creación de un organismo especializado en delitos informáticos para mejorar la coordinación entre las autoridades encargadas de la prevención y persecución de estos delitos y por ultimo una legislación especializada en los diversos ciberdelitos.

---

[21] Hernández-Muñoz, J. L., & Martínez-Ballesteros, A. (2019). El delito informático en la era digital: retos y oportunidades. Cuadernos de Información, 44, 25-37.

En cuanto a la prevención, se sugiere el fortalecimiento de la educación y conciencia cibernética en la población, para que los ciudadanos puedan identificar y prevenir los delitos informáticos. Asimismo, se propone la creación de programas de capacitación especializados para las autoridades encargadas de la investigación y persecución de los delitos informáticos, con el objetivo de mejorar su capacidad para enfrentar estos delitos en un entorno en constante evolución.

En este sentido, según Hernández-Muñoz y Martínez-Ballesteros (2019)[22], la colaboración entre el sector público y privado también es fundamental para la prevención y persecución de delitos informáticos. Por su parte, Berberena (2018)[23] propone la necesidad de promover la cooperación internacional en la lucha contra los delitos informáticos, para combatir el carácter transnacional de estos delitos.

1.7 Legislación actual en México

Después de haber realizado un análisis detallado de los antecedentes de los delitos informáticos en México y específicamente del artículo 211 Bis 1 del Código Penal Federal, se puede concluir que, aunque ha habido avances significativos en la legislación y la aplicación de la ley, aún existen desafíos importantes en la lucha contra estos delitos. La evolución constante de las tecnologías y las nuevas formas de delitos informáticos hacen que la prevención y la persecución de estos delitos sea una tarea cada vez más compleja.

Con base en lo anterior, se recomienda que se continúe investigando en este tema y se realicen esfuerzos para mejorar la legislación y la prevención de los delitos informáticos en México. Es importante que se fomente la colaboración entre los distintos actores involucrados, incluyendo a las autoridades, las empresas, las

[22] Hernández-Muñoz, J. M., & Martínez-Ballesteros, M. (2019). El delito informático en México y su regulación. Cuadernos Electrónicos de Filosofía Del Derecho, (38), 25-43.
[23] Berberena, C. E. (2018). Delitos informáticos: Un reto para la protección de los derechos humanos. Revista Jurídica De La Universidad De Palermo, (26), 47-61.

organizaciones de la sociedad civil y los ciudadanos, para lograr una respuesta efectiva ante estos delitos.

El análisis del artículo 211 Bis 1 del Código Penal Federal es importante porque permite comprender la evolución de la legislación y la aplicación de la ley en materia de delitos informáticos en México. Este artículo es una herramienta fundamental en la lucha contra estos delitos y su aplicación efectiva es clave para prevenir y perseguir los delitos informáticos en el país; asimismo es importante reconocer que aún hay desafíos en la aplicación del artículo y en la prevención de estos delitos, lo que hace necesario continuar trabajando en este tema de manera coordinada y multidisciplinaria.

CAPÍTULO II. CONCEPTOS

En la actualidad, los delitos informáticos se han convertido en una problemática que afecta a nivel mundial. Con el auge de la tecnología y la globalización, se han creado nuevas formas de cometer delitos, y esto ha llevado a una necesidad cada vez mayor de comprender y analizar estos delitos, por esta razón, en este capítulo se abordará el concepto de delito informático, así como los sujetos que intervienen dentro de este tipo de delitos.

Para entender el delito informático es necesario identificar los sujetos que participan en el mismo. El sujeto activo es la persona que comete el delito, mientras que el sujeto pasivo es la víctima del mismo. Además, es importante conocer cuál es la jurisdicción y competencia que corresponde a los casos de delitos informáticos, ya que esto tiene implicaciones significativas en la investigación y en el proceso judicial.

Por ello, este capítulo tiene como objetivo proporcionar una comprensión clara y detallada del concepto de delito informático y los sujetos que intervienen en el mismo, así como la jurisdicción y competencia correspondientes. Este conocimiento es fundamental para entender la naturaleza de los delitos informáticos y para aplicar medidas efectivas en su prevención y persecución.

2. Concepto de Delito Informático

En la era contemporánea, la tecnología y la informática se han convertido en herramientas esenciales en nuestra vida cotidiana, tanto a nivel personal como empresarial. No obstante, esta dependencia también ha traído consigo el aumento de los delitos informáticos, los cuales representan una amenaza constante para la seguridad y privacidad de la información. Por lo tanto, es necesario tener un conocimiento preciso sobre lo que se considera un delito informático y cuáles son los sujetos que intervienen en el mismo.

En esta sección, se abordará el concepto de delito informático, así como los sujetos que intervienen en su comisión y su relación con la jurisdicción y competencia. Con el fin de comprender de manera clara y precisa los aspectos fundamentales de esta temática, se realizará una revisión de las definiciones y conceptos relevantes de la legislación mexicana y comparada. Además, se profundizará en la figura del sujeto activo y pasivo de este tipo de delitos, para entender su dinámica y responsabilidades. Todo ello con el objetivo de brindar una visión completa y detallada del delito informático, una problemática actual y en constante evolución en el ámbito jurídico y tecnológico.

Para entrar en materia, el concepto de delito informático ha sido objeto de discusión y análisis en distintos ámbitos, ya que se trata de un fenómeno relativamente nuevo que ha ido en constante evolución en las últimas décadas. En términos generales, el delito informático se refiere a cualquier actividad ilegal que se comete mediante el uso de tecnologías de la información y la comunicación, como computadoras, internet, dispositivos móviles, entre otros.

De acuerdo con la Asamblea General de la Organización de las Naciones Unidas (ONU) en su Resolución 55/63, se entiende por delito informático a *"cualquier conducta ilícita no ética o no autorizada que se realiza mediante el uso de tecnologías de la información y la comunicación, incluyendo toda conducta que constituya una infracción de las leyes penales que rigen en los Estados miembros"* (Organización de las Naciones Unidas, 2001)[24].

Por su parte, la Unión Europea en su Convenio sobre Ciberdelito establece que el delito informático se refiere a *"cualquier infracción penal de derecho interno que involucre el uso de sistemas de información y comunicación, incluyendo la*

[24] Organización de las Naciones Unidas. (2001). Resolución 55/63 de la Asamblea General: Lucha contra la criminalidad informática. https://undocs.org/es/A/RES/55/63

computadora y la red, cuyo objetivo sea la violación de una ley penal" (Consejo de Europa, 2001)[25].

Estas definiciones ponen de manifiesto la complejidad del concepto de delito informático, ya que no se trata de una categoría delictiva específica, sino de una serie de conductas ilícitas que pueden ser cometidas a través de las tecnologías de la información y la comunicación; asimismo resulta importante destacar que el uso indebido de estas tecnologías puede afectar a diversos ámbitos, tales como la seguridad de la información, la privacidad de los usuarios, el comercio electrónico, entre otros.

En este sentido, el concepto de delito informático se encuentra en constante evolución, debido a que las tecnologías de la información y la comunicación están en constante cambio y desarrollo. Por lo tanto, resulta fundamental que la legislación y las autoridades competentes estén actualizadas y preparadas para hacer frente a los nuevos retos que se presenten en este ámbito.

2.1 Sujetos que intervienen dentro del delito informático

2.1.1 Introducción a los sujetos del delito informático.

Dentro del delito informático, es importante tener en cuenta los diferentes sujetos que pueden estar involucrados. En este sentido, es fundamental mencionar que, a diferencia de otros delitos convencionales, los delitos informáticos pueden tener una gran cantidad de sujetos activos y pasivos, lo que hace que su análisis sea mucho más complejo.

[25] Consejo de Europa. (2001). Convenio sobre Ciberdelito. Recuperado de https://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185

En términos generales, se puede decir que los sujetos que intervienen en los delitos informáticos pueden ser muy diversos y pueden incluir a individuos, empresas, organizaciones y hasta a gobiernos. En este sentido, es importante destacar que el ámbito digital permite una mayor facilidad de acceso a la información y a los sistemas, lo que puede generar una mayor cantidad de sujetos activos y pasivos.

Por otro lado, es importante mencionar que no todos los sujetos involucrados en los delitos informáticos tienen el mismo grado de responsabilidad o participación. De hecho, el papel de cada sujeto puede variar significativamente dependiendo del tipo de delito y de las circunstancias en las que se haya cometido.

De acuerdo con lo anterior, en la investigación sobre el delito informático es fundamental tener en cuenta la complejidad de los sujetos involucrados y su posible implicación en el delito. Como señalan Gómez y Álvarez (2017), *"el estudio de los sujetos activos y pasivos del delito informático es de gran importancia para entender la dinámica del delito y para la elaboración de políticas públicas que permitan su prevención y sanción"*[26].

2.1.2 Autor o agente

Dentro de los sujetos que intervienen en el delito informático, el autor o agente es uno de los más importantes, ya que es quien realiza la acción delictiva, el agente puede ser una persona física o jurídica, y su acción delictiva puede ser tanto activa como pasiva.

En el caso de la acción delictiva activa, el agente realiza una conducta que tiene por objeto infringir la ley, mientras que, en la acción delictiva pasiva, el agente se beneficia de la conducta delictiva de otra persona.

---

[26] Gómez, A., & Álvarez, D. (2017). Delitos informáticos: Análisis de sujetos y problemáticas. Revista de Investigación Académica, 20, 1-14.

Según Vives Antón (2002)[27], el agente del delito informático puede ser una persona física o jurídica, y puede actuar tanto en solitario como en colaboración con otras personas. El autor del delito informático puede ser un hacker, un empleado desleal, un proveedor de servicios de internet, un empresario que busca obtener ventaja competitiva, entre otros.

Es importante señalar que, en muchas ocasiones, el autor del delito informático actúa de forma encubierta y anónima, lo que dificulta su identificación y persecución por parte de las autoridades competentes. En este sentido, es fundamental que la legislación contemple medidas de investigación y persecución eficaces para garantizar la identificación y sanción de los responsables de los delitos informáticos.

2.1.3 Cómplice o cooperador necesario

El cómplice o cooperador necesario es otro sujeto que puede intervenir en el delito informático. Este sujeto colabora directa o indirectamente con el autor o agente en la realización del delito, ya sea antes, durante o después de la comisión del mismo. De acuerdo con el Código Penal Federal mexicano, se considera cómplice a quien presta ayuda o auxilio para la ejecución del delito informático, sin ser autor ni partícipe en su comisión.

En algunos casos, el cómplice puede tener un papel fundamental en la comisión del delito informático, ya que puede brindar apoyo logístico, financiero o tecnológico al autor o agente, lo que permite la realización del delito de manera más efectiva. Sin embargo, también puede ocurrir que el cómplice actúe sin tener conocimiento de que está colaborando en la comisión del delito informático.

[27] Vives Antón, T. (2002). Delitos informáticos: concepto y tipificación. Actualidad Penal, (10), 91-105.

Es importante destacar que la figura del cómplice puede variar dependiendo de la legislación de cada país. Por ejemplo, en algunos países se considera cómplice al sujeto que tiene conocimiento del delito informático y no lo denuncia a las autoridades, mientras que en otros se requiere una colaboración más activa por parte del cómplice.

En definitiva, la intervención del cómplice o cooperador necesario puede ser un elemento clave en la comisión de delitos informáticos y su participación puede ser sancionada de manera similar a la del autor o agente.

De acuerdo con Montiel (2018), *"El cómplice o cooperador necesario es aquel que sin ser autor ni partícipe del delito, coopera de manera necesaria o esencial para su realización, ya sea con actos anteriores, simultáneos o posteriores a la comisión del delito, contribuyendo a la ejecución del mismo"* (p. 43)[28].

2.1.4 Instigador o inductor

El instigador o inductor es otro sujeto que puede intervenir en el delito informático. Según el Código Penal Federal mexicano, se considera como instigador a quien *"con engaños, amenazas, promesas o cualquier otro medio, determine directamente a otro a cometer el delito"* (Código Penal Federal de México, 2021)[29]. En el contexto del delito informático, el instigador puede ser una persona que convence a otra para que cometa el delito o le proporciona información o herramientas para llevarlo a cabo.

La figura del instigador es importante dentro del delito informático, ya que muchas veces se trata de personas con conocimientos técnicos avanzados que pueden manipular a otros para que cometan delitos en línea. En este sentido, el instigador

[28] Montiel, J. (2018). Delitos informáticos: estudio doctrinal y jurisprudencial. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.
[29] Código Penal Federal de México. (2021). Artículo 15. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/9_270621.pdf

puede ser considerado como un "cerebro" del delito, que aprovecha las vulnerabilidades de otros para obtener beneficios.

En cuanto a su responsabilidad penal, el instigador es considerado como autor intelectual del delito y, por lo tanto, puede ser sancionado con la misma pena que el autor material, sin embargo la identificación y persecución del instigador puede ser más complicada que la de otros sujetos, ya que puede actuar de manera oculta o utilizar técnicas de enmascaramiento para evitar ser descubierto.
Por lo tanto, el instigador es un sujeto importante dentro del delito informático, que puede utilizar su conocimiento técnico para manipular a otros y cometer delitos en línea; es necesario prestar atención a esta figura en la prevención y persecución de los delitos informáticos, para poder identificar y sancionar a los responsables.

2.1.5 Beneficiario o receptor de los efectos del delito

El beneficiario o receptor de los efectos del delito es otro sujeto que puede estar involucrado en el delito informático, este sujeto es el que recibe los beneficios directos o indirectos del delito, ya sea económicos o de cualquier otra índole, en algunos casos, este sujeto puede estar relacionado con el sujeto activo o haber instigado el delito.

Según el Código Penal Federal mexicano, el beneficiario o receptor de los efectos del delito puede ser castigado de acuerdo con la gravedad del delito cometido, en su artículo 400 Bis, se establece que *"al que adquiera, enajene, comercie, distribuya, transmita, transporte, procese, almacene, posea, fabrique o introduzca al país, sin contar con la autorización correspondiente, programas informáticos o tecnológicos destinados a cometer delitos, se le impondrá una pena de tres a ocho años de prisión y de cien a trescientos días multa"* (Código Penal Federal de México, 2021)[30].

[30] Código Penal Federal (México). (2021). Última reforma DOF 14-07-2021. https://www.diputados.gob.mx/LeyesBiblio/pdf/9_140721.pdf

Es importante destacar que, en algunos casos, el beneficiario o receptor de los efectos del delito puede ser una persona ajena al delito informático, pero que se beneficia de los resultados del mismo, por ejemplo: un empresario que contrata a un sujeto activo para que realice un ataque informático contra la competencia puede ser considerado beneficiario del delito informático, aunque no haya participado directamente en su comisión.

En este sentido, es fundamental que las legislaciones penales contemplen la figura del beneficiario o receptor de los efectos del delito en el contexto del delito informático, para poder sancionar adecuadamente a todos los sujetos que se benefician de esta actividad delictiva.

2.2 Sujeto activo

2.2.1 Introducción al sujeto activo

El sujeto activo de un delito es la persona que realiza la conducta que está tipificada como delictiva, en el caso de los delitos informáticos, el sujeto activo puede ser cualquier persona que tenga acceso a una computadora o a una red de computadoras y que utilice ese acceso para cometer un delito.

Los delitos informáticos pueden ser cometidos tanto por personas físicas como jurídicas, lo que significa que las empresas también pueden ser consideradas sujetos activos de este tipo de delitos. Por ejemplo, una empresa puede cometer un delito informático al utilizar software pirateado o al utilizar técnicas de hacking para obtener información confidencial de la competencia.

Según el abogado especialista en derecho informático, Manuel David Massón, *"el sujeto activo en los delitos informáticos puede ser cualquier persona que tenga acceso*

a un sistema informático y que utilice ese acceso para realizar una conducta que esté tipificada como delictiva" (Massón, 2015)[31].

En general, la figura del sujeto activo en los delitos informáticos es muy amplia y abarca a cualquier persona o entidad que utilice las tecnologías de la información y la comunicación para cometer una infracción penal, por lo tanto, es importante que las leyes y regulaciones en esta materia estén actualizadas y sean capaces de cubrir todas las posibles situaciones en las que se pueda presentar un delito informático, toda vez que conforme a este señalamiento se desprende que dentro de la dogmática jurídico-penal, estamos en presencia de una calidad especifica del sujeto activo.

2.2.2 Características y tipos de sujetos activos.

Los sujetos activos del delito informático pueden ser muy variados, desde hackers profesionales hasta simples usuarios de Internet que cometen infracciones sin darse cuenta; a continuación se describen algunas de las características y tipos más comunes de sujetos activos en los delitos informáticos.

Uno de los rasgos más notorios de los sujetos activos en el delito informático es su alta especialización en el manejo de tecnologías de la información y la comunicación (TIC). En muchos casos, estos individuos poseen conocimientos avanzados en informática, programación y redes que les permiten llevar a cabo acciones ilegales en línea con gran facilidad y eficacia, al mismo tiempo, algunos delincuentes informáticos pueden ser autodidactas o contar con una formación técnica limitada, pero compensan esta carencia con la habilidad para encontrar vulnerabilidades en sistemas informáticos y explotarlas.

[31] Massón, M. D. (2015). Los delitos informáticos. Cizur Menor: Thomson Reuters Aranzadi.

Otra característica importante de los sujetos activos es su alto grado de anonimato y ocultamiento, en muchos casos, estos individuos operan bajo un pseudónimo o alias que les permite ocultar su verdadera identidad y dificulta su identificación y captura por parte de las autoridades; asimismo los sujetos activos pueden utilizar diversas técnicas y herramientas para proteger su anonimato, como el uso de redes privadas virtuales (VPN), proxies o sistemas de cifrado.

Por otro lado, los sujetos activos en los delitos informáticos pueden clasificarse en diferentes tipos según sus motivaciones y objetivos. Entre los más comunes se encuentran los hackers éticos, que realizan actividades de ciberseguridad y pruebas de penetración con fines legítimos; los crackers o hackers malintencionados, que buscan vulnerar sistemas informáticos con fines ilícitos como el robo de información o el daño a la propiedad; los ciberactivistas, que realizan acciones en línea para promover una causa o ideología determinada; y los cibercriminales organizados, que forman parte de grupos delictivos que se dedican al ciberespionaje, la extorsión o el fraude.

Como se puede apreciar, los sujetos activos del delito informático presentan una amplia variedad de perfiles y características que los hacen un desafío importante para las autoridades y los expertos en ciberseguridad, es fundamental contar con una formación técnica y un conocimiento profundo de las motivaciones y objetivos de estos individuos para poder prevenir y combatir eficazmente los delitos informáticos.

Según Hernández (2014)[32], los sujetos activos en los delitos informáticos pueden ser hackers éticos, crackers, ciberactivistas y cibercriminales organizados, entre otros, además estos individuos se caracterizan por su alta especialización en el manejo de TIC, su grado de anonimato y ocultamiento, y su diversidad de objetivos y motivaciones.

[32] Hernández, R. (2014). Delitos informáticos y seguridad de la información. Pearson Educación.

2.2.3 Delitos informáticos cometidos por hackers

Los hackers son uno de los sujetos activos más conocidos en la comisión de delitos informáticos, los hackers son individuos con habilidades avanzadas en el uso de la tecnología y los sistemas informáticos, y suelen utilizar estas habilidades para acceder a sistemas a los que no tienen autorización o para modificar programas y sistemas con el fin de obtener información o beneficios económicos. Según un estudio de la empresa de seguridad informática Symantec, los hackers pueden clasificarse en tres tipos: los hackers blancos, los hackers grises y los hackers negros (Symantec, 2019)[33].

Los hackers blancos, también conocidos como "sombreros blancos", son expertos en seguridad informática que trabajan para empresas u organizaciones para proteger sus sistemas y redes. Estos hackers suelen realizar pruebas de seguridad y analizar vulnerabilidades para prevenir posibles ataques informáticos, a diferencia de otros tipos de hackers, los hackers blancos operan de manera legal y ética, y están motivados por el desafío y la resolución de problemas.

Los hackers grises, también conocidos como "sombreros grises", tienen habilidades similares a las de los hackers blancos, pero utilizan estas habilidades con fines cuestionables, a diferencia de los hackers negros, los hackers grises no tienen intención de causar daño, pero pueden actuar fuera de los límites éticos y legales en algunos casos.

Los hackers negros, también conocidos como "sombreros negros", son aquellos hackers que utilizan sus habilidades para realizar acciones ilegales o dañinas, estos hackers pueden buscar obtener información personal o financiera de los usuarios, instalar malware o robar información confidencial para luego venderla en el mercado

[33] Symantec. (2019). Understanding Hackers and How They Operate. Recuperado de https://www.symantec.com/content/dam/symantec/docs/reports/understanding-hackers-and-how-they-operate-2019-en.pdf

negro, los hackers negros suelen estar motivados por el lucro y pueden causar daños significativos a los sistemas y redes que atacan.

Es importante destacar que no todos los hackers son delincuentes informáticos, y que el término hacker no debe utilizarse de manera peyorativa para describir a todas las personas con habilidades avanzadas en informática. La mayoría de los hackers utilizan sus habilidades para fines legítimos y éticos, como el desarrollo de software y sistemas de seguridad, sin embargo; es importante tener en cuenta que aquellos hackers que utilizan sus habilidades con fines delictivos pueden causar daños significativos a los sistemas y redes que atacan, y deben ser responsabilizados por sus acciones.

2.2.4 Delitos informáticos cometidos por empleados de la empresa

Los empleados de una empresa también pueden ser sujetos activos de delitos informáticos, ya que tienen acceso a información sensible y a los sistemas informáticos de la compañía. Estos delitos pueden ser cometidos por empleados desleales, que buscan lucrarse a costa de la empresa o dañar su reputación, o por aquellos que desean causar daño por venganza o descontento.

Un ejemplo de este tipo de delito informático es el espionaje corporativo, en el que un empleado accede de forma no autorizada a la información confidencial de la empresa con fines de lucro personal o para beneficiar a otra empresa, también puede darse el caso de que un empleado utilice los recursos informáticos de la compañía para cometer otros delitos informáticos, como la distribución de malware o el phishing.

Es importante destacar que las empresas deben tomar medidas de seguridad para evitar estos delitos, incluyendo la implementación de políticas claras de uso de los recursos informáticos y la limitación del acceso a información confidencial solo a aquellos empleados que necesiten conocerla en el desempeño de sus funciones.

De conformidad con Tapia-Fonllem, en su artículo "Delitos informáticos cometidos por empleados", el hecho de que los empleados tengan acceso a información confidencial y a los sistemas informáticos de la empresa los convierte en un riesgo potencial para la seguridad informática; es por ello que resulta importante que las empresas establezcan medidas de seguridad para prevenir este tipo de delitos, tales como la restricción de accesos y la capacitación de los empleados en el uso seguro de los sistemas informáticos de la empresa (Tapia-Fonllem, 2014)[34].

2.2.5 Delitos informáticos cometidos por terceros

Los delitos informáticos también pueden ser cometidos por terceros que no tienen una relación directa con la víctima o la empresa afectada, estos terceros pueden ser individuos o grupos que buscan obtener beneficios económicos o políticos, o simplemente causar daño o perturbar el normal funcionamiento de los sistemas informáticos.

Entre los delitos informáticos más comunes cometidos por terceros se encuentran el phishing, la distribución de malware, el robo de información y la realización de ataques de denegación de servicio (DDoS); en estos casos, los delincuentes utilizan técnicas avanzadas de ingeniería social y explotan vulnerabilidades en los sistemas informáticos para lograr sus objetivos.

Es importante destacar que los terceros también pueden ser víctimas de los delitos informáticos, como cuando son víctimas de phishing o cuando sus dispositivos son infectados con malware. En estos casos, los delincuentes pueden utilizar la información robada para cometer otros delitos, como el fraude bancario o la suplantación de identidad.

[34] Tapia-Fonllem, C. (2014). Delitos informáticos cometidos por empleados. Investigación y Ciencia, (23), 38-45.

Según Acosta, F. y García, F. (2018), *"los delitos informáticos no solo son realizados por expertos en informática, sino que también pueden ser cometidos por terceros que se valen de recursos informáticos para cometer fraudes y estafas"* (p. 57)[35].

2.3 Sujeto pasivo

2.3.1 Introducción al sujeto pasivo

En el ámbito del derecho penal, el sujeto pasivo es aquel que sufre las consecuencias de un delito, es decir, el objeto material de la acción delictiva, en el caso de los delitos informáticos, el sujeto pasivo puede ser una persona física o jurídica, es decir, una empresa o entidad, que haya sufrido daños o perjuicios a consecuencia de la acción delictiva en el ámbito informático.

Es importante destacar que, en ocasiones, el sujeto pasivo puede no ser una víctima directa de la acción delictiva, sino que puede tratarse de un tercero que se ve afectado indirectamente por las consecuencias de la misma; por ejemplo, en el caso de un ataque informático dirigido a una empresa que almacena datos personales de sus clientes, los clientes de la empresa también pueden ser considerados como sujetos pasivos, ya que sus datos personales se han visto comprometidos y pueden ser utilizados con fines delictivos.

Es fundamental proteger a los sujetos pasivos de los delitos informáticos y garantizar que se hagan responsables a los sujetos activos de las acciones ilícitas que han llevado a cabo. En este sentido, la legislación debe ser lo suficientemente clara para determinar las responsabilidades y sanciones correspondientes en cada caso. Según López-Tarruella Martínez-Conde (2002), el sujeto pasivo del delito informático es *"el*

[35] Acosta, F. y García, F. (2018). Delitos informáticos en México. Revista de Derecho y Ciencias Sociales, 1(1), 51-68.

destinatario final de la conducta que el autor realiza a través de la informática" (p. 168)[36].

Además, los sujetos pasivos de los delitos informáticos pueden ser tanto personas físicas como jurídicas, en el caso de las personas físicas, pueden ser tanto usuarios particulares como trabajadores de una empresa o institución que hayan sido víctimas de un delito informático; para señalar por ejemplo de las personas jurídicas, pueden ser empresas, organizaciones no gubernamentales, gobiernos, entre otros.

Es importante destacar que, en muchas ocasiones, los sujetos pasivos de los delitos informáticos son víctimas indirectas, es decir, pueden sufrir las consecuencias del delito informático sin haber sido el objetivo principal del ataque, por ejemplo, en el caso de un ataque informático dirigido a una empresa para obtener información confidencial, los clientes de dicha empresa también pueden resultar afectados si sus datos personales han sido robados o comprometidos.

En definitiva, el sujeto pasivo de los delitos informáticos es fundamental en la definición de este tipo de delitos, ya que sin una víctima no puede haber delito. Por lo tanto, es importante que las legislaciones y las políticas públicas estén enfocadas en proteger a los sujetos pasivos de los delitos informáticos y en establecer medidas efectivas para prevenir y combatir este tipo de delitos.

2.3.2 Características y tipos de sujetos pasivos

En el contexto de los delitos informáticos, el sujeto pasivo se refiere a la persona o entidad que sufre la consecuencia perjudicial del delito, puede ser una persona física o jurídica y puede verse afectada de diversas maneras, como la pérdida de información, la interrupción del servicio o la violación de la privacidad.

---

[36] López-Tarruella Martínez-Conde, E. (2002). Delitos informáticos: concepto y regulación. Revista Electrónica de Estudios Jurídicos, (1), 1-23.

Los sujetos pasivos de los delitos informáticos pueden ser clasificados en varios tipos según su relación con el delincuente. Uno de ellos son los sujetos pasivos directos, que son aquellos que sufren el daño directamente por la acción del delincuente. Por ejemplo, un usuario cuya información personal ha sido robada o una empresa cuyo sistema ha sido infectado por un virus informático.

Otro tipo de sujetos pasivos son los indirectos, que son aquellos que no sufren directamente la acción del delincuente, pero pueden verse afectados por sus consecuencias. Por ejemplo, los clientes de una empresa cuyo sistema ha sido infectado y se ha interrumpido el servicio.

Además, también existen sujetos pasivos colectivos, que son aquellos que representan a un grupo de personas o entidades que han sido afectados por el mismo delito informático. Por ejemplo, una asociación que representa a varias empresas que han sufrido el mismo ataque informático.

Por lo tanto, los sujetos pasivos de los delitos informáticos pueden ser de diferentes tipos y se ven afectados de diversas maneras, es importante tener en cuenta su papel en la comisión y las consecuencias de estos delitos para poder prevenirlos y sancionarlos adecuadamente.

Además de los sujetos pasivos mencionados anteriormente, es importante destacar que también pueden ser víctimas de los delitos informáticos personas físicas o jurídicas que no tienen una relación directa con el sujeto activo. Por ejemplo, en el caso de la difusión no autorizada de información privada en internet, la víctima puede ser cualquier persona que tenga su información expuesta sin su consentimiento.

Entonces, los sujetos pasivos de los delitos informáticos son muy diversos y van desde personas físicas o jurídicas relacionadas directamente con el sujeto activo hasta terceros que resultan afectados de manera indirecta por los actos delictivos, es importante destacar que, en muchos casos, los delitos informáticos pueden tener un

impacto a gran escala y afectar a numerosas personas y organizaciones, por lo que es fundamental tomar medidas preventivas y reforzar la seguridad en el entorno digital.

2.3.3 Delitos informáticos cometidos contra el gobierno.

Los delitos informáticos cometidos contra el gobierno son una de las categorías de sujetos pasivos en este tipo de delitos, en este caso, los delincuentes informáticos buscan afectar la seguridad o la confidencialidad de los datos y sistemas de las instituciones gubernamentales.

Entre los delitos informáticos cometidos contra el gobierno se pueden incluir la interceptación y el acceso no autorizado a datos gubernamentales, la modificación o destrucción de información gubernamental, la interferencia con servicios públicos y la difusión de información falsa con el objetivo de perjudicar la imagen del gobierno o generar caos social.

Es importante señalar que estos delitos pueden tener graves consecuencias, no solo para las instituciones gubernamentales afectadas, sino también para la sociedad en general, ya que pueden poner en riesgo la seguridad nacional, la estabilidad política y la privacidad de los ciudadanos. Según López-Tarruella Martínez-Conde (2002)[37], los delitos informáticos contra el gobierno pueden ser cometidos por actores nacionales o internacionales y pueden tener motivaciones políticas, económicas o ideológicas, ya que es fundamental que las instituciones gubernamentales adopten medidas preventivas y de protección para minimizar los riesgos de este tipo de delitos y para poder actuar de manera efectiva en caso de ser víctimas de los mismos.

[37] López-Tarruella Martínez-Conde, O. (2002). Los delitos informáticos. Editorial Comares.

2.3.4 Delitos informáticos cometidos contra empresas.

Los delitos informáticos cometidos contra empresas son una realidad cada vez más frecuente en la actualidad, especialmente en un mundo donde la tecnología es cada vez más importante en el ámbito empresarial. Los sujetos activos de estos delitos suelen ser hackers, empleados desleales o terceros malintencionados, y sus objetivos pueden variar desde obtener información confidencial hasta realizar sabotajes o extorsiones.

Estos delitos pueden tener consecuencias económicas y de reputación muy graves para las empresas afectadas, y a menudo se requiere la intervención de expertos en seguridad informática para investigar y resolver estos problemas.

Según Miquel Peguera (2018)[38], los delitos informáticos cometidos contra empresas pueden tener diversas formas, como el robo de información confidencial, la suplantación de identidad, el sabotaje a sistemas informáticos, la extorsión y el secuestro de datos. Estos delitos pueden ser realizados por hackers, empleados desleales o incluso competidores comerciales.

Además de las empresas dedicadas a la tecnología de la información, las organizaciones en otros sectores también pueden ser víctimas de delitos informáticos. Por ejemplo, las empresas financieras son un objetivo común debido a la gran cantidad de información confidencial que manejan, como datos de clientes y transacciones financieras, del mismo modo, las empresas de servicios de salud son vulnerables debido a la gran cantidad de información médica confidencial que poseen.

Por ello, los delitos informáticos pueden ser cometidos contra una amplia variedad de sujetos pasivos, incluyendo individuos, gobiernos, empresas y organizaciones, los

[38] Peguera, M. (2018). Cibercrimen y derecho: Los delitos informáticos en la sociedad de la información. Aranzadi.

sujetos pasivos pueden sufrir una amplia gama de daños, desde la pérdida de información confidencial hasta la interrupción de los servicios y la pérdida financiera. Es esencial que estos sujetos pasivos tomen medidas para protegerse contra los delitos informáticos y mitigar los daños en caso de que ocurran.

2.3.5 Delitos informáticos cometidos contra personas físicas

Los delitos informáticos también pueden ser cometidos contra personas físicas, como individuos o grupos de personas, en este caso, los sujetos pasivos son aquellas personas que son víctimas de los delitos informáticos, y pueden ser afectadas de diversas maneras; por ejemplo, pueden sufrir robo de identidad, acoso en línea, extorsión o fraude en línea.

Según un estudio sobre el impacto de los delitos informáticos en las personas físicas realizado por la Organización de los Estados Americanos (OEA), se encontró que las personas afectadas por estos delitos pueden experimentar una serie de efectos negativos en su vida diaria. Algunos de estos efectos incluyen *"pérdida de información personal, financiera y profesional, impacto emocional, problemas de salud mental y, en algunos casos, amenazas a la seguridad física"* (OEA, 2016, p. 3)[39].

Es importante destacar que los delitos informáticos cometidos contra personas físicas no solo afectan a las víctimas directas, sino también a su entorno cercano. Por ejemplo, si un individuo sufre robo de identidad, esto puede tener un impacto en su familia y amigos cercanos.

En cuanto a las características de los sujetos pasivos en los delitos informáticos contra personas físicas, se puede decir que estos son individuos que utilizan la tecnología en su vida diaria y se convierten en víctimas de los delitos informáticos. Según López-

[39] Organización de los Estados Americanos. (2016). Estudio sobre el impacto de los delitos informáticos en las personas. Recuperado de https://www.oas.org/juridico/spanish/cyb_estudio_delitos_informaticos_personas.pdf

Tarruella y Martínez-Conde (2002), los sujetos pasivos de los delitos informáticos son *"personas físicas o jurídicas que sufren las consecuencias del delito, tales como la pérdida de datos, la interrupción de servicios o la violación de la privacidad"* (p. 28)[40].

En este sentido, es importante destacar que los delitos informáticos contra personas físicas pueden tener consecuencias graves en la vida de las víctimas, incluyendo daños emocionales, financieros y de reputación, es por ello que se requiere una mayor conciencia y prevención en este ámbito, así como una legislación adecuada y herramientas de protección para las personas físicas afectadas por los delitos informáticos.

2.4 Jurisdicción y competencia

2.4.1 Introducción a la jurisdicción y competencia

La jurisdicción y competencia son conceptos fundamentales en cualquier proceso judicial, y el ámbito de los delitos informáticos no es una excepción. La jurisdicción se refiere al poder que tiene un tribunal para conocer y decidir un caso, mientras que la competencia se refiere a la capacidad de un tribunal para ejercer esa jurisdicción en un caso específico.

En el ámbito de los delitos informáticos, la jurisdicción y la competencia pueden ser especialmente complicadas debido a la naturaleza transfronteriza de muchos de estos delitos. Por ejemplo, un delito informático puede ser cometido desde un país, pero tener consecuencias en otro país, además los delitos informáticos pueden implicar la violación de leyes nacionales e internacionales, lo que añade otra capa de complejidad a la cuestión de la jurisdicción y competencia.

[40] López-Tarruella Martínez-Conde, E. (2002). Delitos informáticos. Marcial Pons.

En este sentido, hay diferentes acuerdos internacionales que pueden ser utilizados para ayudar a resolver conflictos de jurisdicción y competencia en los casos de delitos informáticos. Por ejemplo, la Convención de Budapest sobre Ciberdelitos establece una serie de medidas para la cooperación internacional en la investigación y persecución de los delitos informáticos, incluyendo la resolución de conflictos de jurisdicción y competencia.

Es importante tener en cuenta que la jurisdicción y competencia en los casos de delitos informáticos pueden ser influenciadas por diferentes factores, como la ubicación de los servidores o el lugar donde se produjo el daño. Por lo tanto, es fundamental que los investigadores y los tribunales tengan un buen entendimiento de la jurisdicción y competencia en el ámbito de los delitos informáticos.

Como señalan López-Tarruella y Martínez-Conde (2002), *"la jurisdicción y competencia en materia de delitos informáticos son complejas debido a la naturaleza transnacional de estos delitos, la falta de consenso internacional sobre el alcance de las leyes y la falta de armonización entre los sistemas legales de diferentes países"* (p. 89)[41]. Por lo tanto, es fundamental contar con acuerdos y mecanismos internacionales que permitan la cooperación y el trabajo conjunto entre los países para garantizar la efectiva persecución de los delitos informáticos.

2.4.2 Competencia territorial

La competencia territorial se refiere a la delimitación geográfica en la que un determinado tribunal tiene la facultad de ejercer su jurisdicción y dictar sentencias, en el ámbito del derecho penal, la competencia territorial es de especial importancia ya que determina cuál es el tribunal encargado de juzgar un delito y cuál es la ley aplicable.

[41] López-Tarruella Martínez-Conde, E. (2002). El tratamiento penal de los delitos informáticos. Bosch.

En el caso de los delitos informáticos, la competencia territorial puede ser especialmente compleja debido a la naturaleza transnacional de muchas de estas conductas, en algunos casos, un delito informático puede haber sido cometido en un país, pero tener efectos en otros, o bien puede haber sido perpetrado desde un país diferente al de la víctima o el servidor afectado, por esta razón, la determinación de la competencia territorial en el ámbito de los delitos informáticos puede resultar complicada y generar conflictos entre distintas jurisdicciones.

Según López-Tarruella, la determinación de la competencia territorial en los delitos informáticos debe realizarse atendiendo a diversos criterios, tales como *"el lugar en que se haya cometido la conducta, el lugar en que se haya producido el resultado, el lugar donde se encuentren las pruebas y el lugar donde residan las víctimas o los sujetos pasivos de la conducta"* (López-Tarruella, 2002, p. 156)[42]. En este sentido, es importante tener en cuenta que, en algunos casos, la competencia territorial puede ser concurrente, es decir, que varios tribunales tienen la facultad de juzgar un mismo delito.

2.4.3 Competencia material

La competencia material se refiere a la atribución de un órgano jurisdiccional para conocer de un determinado tipo de delito. En el ámbito de los delitos informáticos, esta competencia se encuentra establecida en la legislación de cada país, y puede variar según la naturaleza del delito y la jurisdicción correspondiente.

Por ejemplo, en España, la Ley Orgánica 10/1995 del Código Penal establece en su artículo 23 que los juzgados y tribunales españoles serán competentes para conocer de los delitos cometidos en territorio español o por españoles o extranjeros fuera de España, cuando el delito esté tipificado como delito en la legislación española.

---

[42] López-Tarruella Martínez-Conde, A. (2002). Jurisdicción y competencia en los delitos informáticos. Revista General de Derecho Penal, (2), 155-176.

Es importante destacar que, en el caso de delitos informáticos, la competencia material puede ser compleja debido a la naturaleza transnacional de este tipo de delitos; es decir, un delito informático puede ser cometido desde un país distinto al del sujeto activo o pasivo, lo que puede implicar la intervención de diferentes órganos jurisdiccionales de distintos países.

En este sentido, se hace necesario que los diferentes países establezcan acuerdos y mecanismos de cooperación para garantizar una eficaz lucha contra los delitos informáticos a nivel internacional.

De acuerdo con lo anterior, la importancia de la competencia material en los delitos informáticos radica en que permite determinar qué órgano jurisdiccional es competente para conocer de un determinado caso, lo que garantiza un proceso justo y eficaz.

2.4.4 Competencia funcional

La competencia funcional se refiere a la atribución de las funciones y competencias que corresponden a cada órgano judicial, en el caso de los delitos informáticos, esta competencia puede depender del tipo de delito cometido, así como de la categoría del sujeto activo o pasivo involucrado. Por ejemplo, un delito informático cometido por un menor de edad puede ser competencia de un juzgado de menores, mientras que un delito informático de carácter internacional puede requerir la intervención de autoridades de distintos países.

Es importante tener en cuenta que, debido a la complejidad y la rapidez con que se desarrollan los delitos informáticos, es fundamental que las autoridades judiciales tengan un alto grado de especialización y conocimiento en el ámbito de la informática y las tecnologías de la información, en muchos países, se han establecido unidades especializadas en delitos informáticos en las fuerzas de seguridad y en los órganos judiciales, con el objetivo de abordar de manera más efectiva estos tipos de delitos.

En cuanto a la competencia funcional específica en el ámbito de los delitos informáticos, López-Tarruella y Martínez-Conde (2002) señalan que *"la competencia funcional en materia de delitos informáticos dependerá del tipo de delito de que se trate, del órgano judicial que corresponda en virtud de las normas de reparto de competencias y de los acuerdos adoptados en el seno de las autoridades judiciales"* (p. 30)[43].

2.4.5 Conflictos de jurisdicción y competencia en el delito informático.

El delito informático puede presentar conflictos de jurisdicción y competencia debido a la naturaleza transfronteriza de las redes de computadoras y la falta de armonización de las leyes entre los países, en casos de delitos informáticos internacionales, puede ser difícil determinar qué país tiene jurisdicción y competencia para enjuiciar al acusado.

En la mayoría de los casos, la jurisdicción se determina por el lugar donde se cometió el delito, donde se produjeron los efectos del delito y donde se encuentra el acusado, sin embargo, en casos de delitos informáticos, estos factores pueden ser difíciles de determinar y pueden surgir conflictos de jurisdicción y competencia entre diferentes países.

Para resolver estos conflictos, los países pueden tener que recurrir a tratados internacionales y acuerdos de cooperación judicial. Estos acuerdos establecen las reglas y procedimientos para la extradición de los acusados, la transferencia de pruebas y la cooperación entre los países en la investigación y enjuiciamiento de los delitos informáticos.

[43] López-Tarruella Martínez-Conde, P. (2002). Delitos informáticos y propiedad intelectual. Dykinson.

Por lo tanto, los conflictos de jurisdicción y competencia en el delito informático son comunes debido a la naturaleza transfronteriza de los delitos informáticos, la resolución de estos conflictos puede requerir la cooperación internacional y el cumplimiento de los acuerdos internacionales en materia de cooperación judicial.

En estos casos, los tribunales deberán determinar la jurisdicción y competencia correspondiente para llevar a cabo el proceso penal. De acuerdo con la Ley de Enjuiciamiento Criminal española, en caso de conflictos de jurisdicción, los tribunales superiores de justicia deberán resolverlos, además, en caso de que se suscite un conflicto de competencia entre dos juzgados o tribunales, se aplicarán los criterios establecidos en la propia ley para resolver el conflicto.

En el ámbito internacional, la determinación de la jurisdicción y competencia puede ser aún más compleja debido a la existencia de distintos ordenamientos jurídicos y a la dificultad para identificar al autor del delito informático, que puede encontrarse en otro país. En estos casos, se aplican los tratados internacionales y las normativas de cada país para determinar la jurisdicción y competencia correspondiente.

Es importante destacar que la jurisdicción y competencia deben ser determinadas de manera precisa y adecuada, ya que de ello depende la correcta aplicación de la ley y la justa resolución del caso. Además, la determinación correcta de la jurisdicción y competencia puede tener un impacto significativo en la eficacia y rapidez del proceso penal.

CAPÍTULO.III. DELITO: ELEMENTOS

3.1 Antijuridicidad

La antijuridicidad es uno de los elementos esenciales del delito, que se refiere a la contrariedad de la conducta del autor con el ordenamiento jurídico establecido, en el contexto de los delitos informáticos, la antijuridicidad implica que la conducta realizada por el autor del delito informático sea contraria a las normas y regulaciones vigentes en el ámbito legal, específicamente en relación con el uso de la tecnología de la información y las comunicaciones.

Los delitos informáticos son conductas delictivas que se cometen utilizando la tecnología informática como medio o fin para la realización de actividades ilícitas. Estos delitos pueden incluir el acceso no autorizado a sistemas informáticos, la interceptación ilegal de datos, el sabotaje informático, la difusión de malware, la estafa en línea, entre otros, en este sentido, el análisis de la antijuridicidad en el contexto de los delitos informáticos implica examinar cómo la conducta del autor se ajusta o no a las normas legales aplicables en materia de informática y protección de datos.

Es importante tener en cuenta que la tecnología informática avanza rápidamente, lo que plantea desafíos constantes para la legislación y la interpretación de la antijuridicidad en el contexto de los delitos informáticos. En palabras de Laura Mayer Lux (2018) *"el desarrollo que constantemente experimenta la informática supone numerosas modificaciones en periodos muy breves de tiempo. Pues bien, tanto los legisladores como los operadores del sistema procesal penal (jueces, fiscales, defensores) y la doctrina especializada se ven en la necesidad de enfrentar este ámbito multidisciplinar del saber, comprender sus rasgos esenciales y adaptar su labor a una realidad en continuo cambio"*. Por lo tanto, la falta de regulaciones específicas y la complejidad técnica de estos delitos pueden generar debates y controversias en la determinación de la antijuridicidad de la conducta.

En el análisis de la antijuridicidad en el contexto de los delitos informáticos, se deben considerar varios aspectos; en primer lugar, es necesario examinar las normas penales aplicables en cada jurisdicción, así como las regulaciones específicas en materia de tecnologías de la información y la protección de datos, esto incluye el estudio detallado de los códigos penales, leyes de protección de datos, leyes de ciberseguridad y otras normativas relevantes que establecen los límites legales en el uso de la tecnología informática.

Asimismo, es importante analizar la jurisprudencia y la doctrina relacionada con la antijuridicidad en el contexto de los delitos informáticos. La interpretación de los tribunales y la evolución de la jurisprudencia en este ámbito pueden brindar orientación sobre cómo se ha abordado y se aborda actualmente la antijuridicidad en casos de delitos informáticos.

Además, el análisis de la antijuridicidad en el contexto de los delitos informáticos debe considerar los tratados internacionales relevantes en materia de ciberdelincuencia. Estos tratados, como el Convenio de Budapest del Consejo de Europa y la Convención de las Naciones Unidas sobre Delitos Informáticos, establecen normas y principios internacionales para la prevención, persecución y sanción de los delitos informáticos, incluyendo la antijuridicidad de la conducta.

En este sentido, la antijuridicidad en el contexto de los delitos informáticos no solo se refiere a la contradicción de la conducta del autor con las normas y regulaciones legales, sino también con los principios éticos y morales en el uso de la tecnología informática, por ejemplo, el acceso no autorizado a sistemas informáticos o la difusión de malware puede ser antijurídico tanto desde una perspectiva legal como ética, ya que viola la privacidad, la confidencialidad y la integridad de la información de terceros.

Es importante mencionar que la antijuridicidad en el contexto de los delitos informáticos puede ser evaluada de manera objetiva y subjetiva. Desde un enfoque objetivo, se evalúa si la conducta del autor es contraria a las normas legales y regulaciones

vigentes en el ámbito informático, independientemente de la intención o conocimiento del autor sobre la ilegalidad de su actuar, por otro lado, desde un enfoque subjetivo, se evalúa si el autor tenía conocimiento de la ilegalidad de su conducta y, a pesar de ello, la realizó voluntariamente.

En este contexto, algunos autores sostienen que la antijuridicidad en los delitos informáticos debe ser evaluada desde una perspectiva más amplia que la mera contradicción con las normas legales, por ejemplo, según un artículo de la UNAM (s.f.), se argumenta que en el análisis de la antijuridicidad de los delitos informáticos se deben tener en cuenta los principios de proporcionalidad y subsidiariedad, así como los intereses en juego, como la seguridad informática, la protección de datos, la libertad de expresión y otros derechos fundamentales.

En el contexto de los delitos informáticos, como el acceso no autorizado y el fraude electrónico, la antijuridicidad se refiere a la falta de conformidad de la conducta del autor con las normas y regulaciones legales aplicables. Estos delitos involucran acciones ilícitas que se llevan a cabo a través de medios electrónicos o informáticos, y su antijuridicidad se establece en base a la contravención de las leyes y regulaciones específicas que rigen el uso y acceso a sistemas, redes, datos o información electrónica. Como señala Acurio Del Pino (s.f.), la criminalidad mediante computadoras *“se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.”.*

En el caso del acceso no autorizado, la antijuridicidad se establece cuando una persona obtiene acceso a un sistema informático o red sin la debida autorización, esto puede involucrar el ingreso a un sistema protegido mediante el uso de contraseñas o credenciales de acceso obtenidas de manera ilícita, la vulneración de medidas de seguridad, el bypass de restricciones de acceso, o la obtención de información sensible o confidencial sin la debida autorización.

La antijuridicidad se establece en base a las leyes y regulaciones que prohíben el acceso no autorizado a sistemas informáticos, protegiendo la integridad, confidencialidad y disponibilidad de la información almacenada en dichos sistemas, en el caso del fraude electrónico, la antijuridicidad se establece cuando una persona utiliza medios electrónicos o informáticos para cometer fraude, engaño o decepción con el fin de obtener un beneficio económico o causar perjuicio a otra persona o entidad.

Esto puede involucrar la manipulación de datos o información electrónica, la falsificación de identidades, el robo de datos financieros, la suplantación de identidad, la creación de páginas web falsas, el phishing, o cualquier otra acción fraudulenta realizada a través de medios electrónicos, la antijuridicidad se establece en base a las leyes y regulaciones que prohíben el fraude electrónico, protegiendo la confianza en el uso de la tecnología informática y las transacciones electrónicas.

Es importante mencionar que la antijuridicidad en estos delitos informáticos puede ser evaluada de manera objetiva y subjetiva. Desde un enfoque objetivo, se evalúa si la conducta del autor se ajusta a las normas legales y regulaciones específicas que prohíben el acceso no autorizado o el fraude electrónico, independientemente de la intención o conocimiento del autor sobre la ilegalidad de su actuar, por otro lado, desde un enfoque subjetivo, se evalúa si el autor tenía conocimiento de la ilegalidad de su conducta y, a pesar de ello, la realizó voluntariamente.

3.2 Culpabilidad

La culpabilidad es uno de los elementos fundamentales del delito, que se refiere a la imputabilidad moral y psicológica del autor de la conducta delictiva, en el contexto de los delitos informáticos, la reflexión sobre los elementos de culpabilidad adquiere particular relevancia debido a las características propias de este tipo de delitos, que suelen involucrar un alto grado de sofisticación tecnológica y complejidad en su comisión.

En primer lugar, es importante tener en cuenta que la culpabilidad en los delitos informáticos se evalúa de acuerdo a los principios generales del derecho penal, que establecen que para que una persona sea culpable de un delito, debe haber actuado con conocimiento y voluntad; esto implica que: el autor del delito informático debe tener conocimiento de la ilegalidad de su conducta y actuar de forma voluntaria, es decir, con la intención de realizar la conducta delictiva o con la conciencia de que está llevando a cabo una acción prohibida por la ley. Según la publicación del blog de Mya Jurídico (2022), *"La culpabilidad se compone por tres elementos, (1) la imputabilidad, (2) la conciencia de la antijuridicidad, (3) la exigibilidad de otra conducta, cuando falta alguno de estos requisitos no puede existir culpabilidad y por ende no se puede imponer una pena."*

En el contexto de los delitos informáticos, la reflexión sobre la culpabilidad puede abordar diferentes aspectos, tales como:

- Conocimiento sobre la ilicitud de la conducta: Dado que los delitos informáticos suelen involucrar acciones realizadas a través de medios electrónicos o informáticos, es necesario evaluar si el autor tenía conocimiento de la ilicitud de su conducta. Esto implica analizar si el autor sabía que estaba vulnerando sistemas de seguridad, accediendo de forma no autorizada a datos o información, o realizando acciones fraudulentas a través de medios electrónicos.

- Voluntad de cometer la conducta: La voluntad del autor de cometer la conducta delictiva es un elemento esencial de la culpabilidad en los delitos informáticos. Esto implica evaluar si el autor actuó de forma voluntaria y consciente, con la intención de llevar a cabo la conducta delictiva. Por ejemplo, si el autor realizó una acción informática con plena conciencia de que estaba infringiendo la ley o causando perjuicio a otra persona o entidad.

- Nivel de conocimiento técnico: En muchos casos, los delitos informáticos requieren un alto nivel de conocimiento técnico en el uso de tecnologías informáticas

y sistemas electrónicos, por lo tanto, es relevante evaluar si el autor tenía el conocimiento técnico necesario para llevar a cabo la conducta delictiva. Esto puede incluir el conocimiento de programación, hacking, técnicas de encriptación, entre otros.

- Grado de participación: En algunos delitos informáticos, puede existir la participación de varias personas, ya sea de forma directa o indirecta. En este caso, es necesario reflexionar sobre el grado de culpabilidad de cada uno de los participantes, evaluando su nivel de conocimiento, voluntad y participación en la conducta delictiva.

Por otra parte, la imputabilidad y el conocimiento del autor son aspectos fundamentales en la evaluación de la culpabilidad en el ámbito digital en el contexto de los delitos informáticos, la imputabilidad se refiere a la capacidad del autor de comprender la naturaleza y consecuencias de sus actos, así como de dirigir su conducta de acuerdo a esa comprensión; en consecuencia el conocimiento del autor se refiere a su nivel de familiaridad y comprensión de las tecnologías informáticas y su capacidad de entender las implicaciones legales y éticas de sus acciones en el entorno digital.

Es importante considerar que los delitos informáticos suelen implicar el uso de tecnologías avanzadas y conocimientos técnicos especializados, por lo tanto, la imputabilidad y el conocimiento del autor en el ámbito digital son aspectos relevantes para evaluar su culpabilidad en la comisión de un delito informático.

En este sentido, se debe tener en cuenta que la imputabilidad en el ámbito digital se rige por los mismos principios generales del derecho penal que en el ámbito tradicional. Es decir, se evalúa la capacidad mental del autor al momento de cometer el delito, considerando factores como la edad, salud mental, y la influencia de sustancias psicoactivas, entre otros; además, se debe considerar si el autor tenía la capacidad de comprender la ilicitud de su conducta y si pudo actuar de acuerdo a esa comprensión, por ejemplo, si el autor tenía conocimiento previo de las leyes y regulaciones que rigen el uso de tecnologías informáticas y aun así decidió cometer el delito, se podría inferir una mayor culpabilidad.

Por otro lado, el conocimiento del autor en el ámbito digital es un factor relevante para evaluar su culpabilidad en delitos informáticos, se debe considerar si el autor tenía un nivel de conocimiento técnico suficiente para comprender la naturaleza y consecuencias de sus actos en el entorno digital, por ejemplo, si el delito informático implicaba el uso de técnicas de hacking, programación, encriptación u otras habilidades técnicas especializadas, se deberá evaluar si el autor tenía el conocimiento necesario para llevar a cabo dicha conducta.

Es importante tener en cuenta que la evaluación de la imputabilidad y el conocimiento del autor en el ámbito digital puede ser compleja, ya que las tecnologías informáticas evolucionan rápidamente y los conocimientos técnicos necesarios para cometer delitos informáticos pueden variar en cada caso. Además, el marco legal y jurisprudencial en materia de delitos informáticos también puede variar de un país a otro, lo que hace necesario un análisis detallado y contextualizado en cada caso.

- Exculpación y atenuación de la culpabilidad en delitos informáticos, como el dolo y la negligencia en el uso de tecnología

La exculpación y atenuación de la culpabilidad son elementos relevantes en la evaluación de la culpabilidad en el contexto de los delitos informáticos, especialmente en lo que respecta al dolo y la negligencia en el uso de la tecnología.

El dolo es una forma de culpabilidad que implica la intención deliberada de cometer un delito, en el ámbito de los delitos informáticos, el dolo se puede manifestar en la realización consciente y voluntaria de actos ilegales utilizando tecnologías informáticas. Por ejemplo, un individuo que intencionalmente accede sin autorización a un sistema informático con el propósito de robar información confidencial o causar daño a un tercero, actúa con dolo en la comisión del delito informático.

En el contexto de los delitos informáticos, la exculpación del dolo puede ocurrir en situaciones donde el autor no tenía conocimiento o comprensión suficiente de la naturaleza ilícita de sus actos, por ejemplo, si un individuo realiza una acción que

puede ser considerada un delito informático, pero lo hace bajo una creencia errónea de que tenía el derecho legal o autorización para realizar dicha acción, podría argumentar que carecía de dolo debido a su falta de conocimiento o comprensión sobre la ilicitud de su conducta.

Sin embargo, es importante tener en cuenta que la ignorancia o el desconocimiento de las leyes no eximen automáticamente de la culpabilidad en delitos informáticos, y la exculpación del dolo en el contexto digital debe evaluarse cuidadosamente en cada caso, considerando las circunstancias específicas.

La negligencia es otra forma de culpabilidad que puede ser relevante en delitos informáticos. La negligencia implica la falta de cuidado o atención debida en el uso de la tecnología, lo que resulta en la comisión de un delito, por ejemplo, si un individuo descuida las medidas de seguridad adecuadas en su sistema informático y permite el acceso no autorizado a terceros, causando daños, podría ser considerado culpable por negligencia en la comisión de un delito informático.

En el contexto de los delitos informáticos, la atenuación de la culpabilidad por negligencia puede ocurrir en situaciones donde el autor ha tomado medidas razonables para proteger su sistema informático, pero aun así se ha producido el acceso no autorizado o el delito informático.

Por ejemplo, si un individuo ha implementado medidas de seguridad actualizadas y sofisticadas en su sistema informático, pero el delito informático se lleva a cabo mediante una brecha de seguridad imprevista o una vulnerabilidad desconocida, se podría argumentar que la culpabilidad del autor debe ser atenuada debido a su diligencia razonable en la protección de su sistema.

Según la Legislación SCJN (s.f.), *"la figura típica de que se trate, será la base del tipo penal del delito doloso o culposo al que la misma se refiera, el que podrá ampliarse por las modalidades agravantes o atenuantes que la ley vincule a ese tipo penal, así*

como modificarse o ampliarse por conductas de autoría distintas a las de autores materiales, así como a través de otras formas de intervención típica dolosa, si se trata de un delito doloso, o bien por conductas de terceros responsables si se trata de un delito culposo".

Por lo tanto, es importante tener en cuenta que la exculpación o atenuación de la culpabilidad en delitos informáticos basada en el dolo o la negligencia debe ser evaluada cuidadosamente en cada caso, considerando las circunstancias específicas y la legislación aplicable.

Figura 1. Diferencia entre delito doloso y culposo.

Fuente: Instituto Latinoamericano de Capacitaciones Jurídicas-ILCJ (2022).

3.3 Imputabilidad del sujeto

El análisis de la capacidad de comprensión y voluntad del autor es un elemento relevante en la evaluación de la imputabilidad del sujeto en el contexto de los delitos informáticos; la imputabilidad se refiere a la capacidad del individuo de comprender la naturaleza y consecuencias de sus acciones y actuar de manera voluntaria y consciente al cometer un delito.

En el ámbito de los delitos informáticos, la capacidad de comprensión se refiere a la capacidad del autor de entender la naturaleza y las implicaciones legales de su conducta. Esto implica tener un nivel adecuado de conocimiento sobre las tecnologías informáticas utilizadas, así como la comprensión de las leyes y regulaciones que rigen el uso de dichas tecnologías. Por ejemplo, un individuo que realiza un ataque cibernético para robar información confidencial de una empresa debe tener la capacidad de comprender la ilegalidad de sus acciones y las posibles consecuencias legales.

La capacidad de voluntad se refiere a la capacidad del autor de actuar de manera voluntaria y consciente al cometer un delito, esto implica tener la capacidad de tomar decisiones libres y conscientes sin ser coaccionado o influenciado indebidamente por terceros, en el contexto de los delitos informáticos, la capacidad de voluntad puede verse afectada por factores como la presión de grupo, la influencia de la cultura de Internet, la adicción a la tecnología u otros factores psicológicos que pueden influir en la capacidad del autor para actuar de manera autónoma y consciente.

Es importante tener en cuenta que el análisis de la capacidad de comprensión y voluntad del autor en delitos informáticos puede ser complejo debido a la naturaleza especializada de las tecnologías informáticas y la rápida evolución de este campo. Es necesario evaluar cuidadosamente la capacidad de comprensión y voluntad del autor en cada caso, considerando las circunstancias específicas, la legislación aplicable y la evidencia disponible, incluyendo pruebas psicológicas y psiquiátricas si es necesario.

La imputabilidad del sujeto en el contexto de los delitos informáticos también puede verse afectada por la edad del autor. En algunos países, la edad legal de imputabilidad puede ser diferente para los delitos informáticos en comparación con otros delitos. Por ejemplo, algunos países pueden tener una edad legal de imputabilidad menor para delitos informáticos debido a la complejidad y la naturaleza especializada de estos delitos.

En el caso de México, según un artículo de la Escuela Judicial del Consejo de la Judicatura Federal (2019), *"es necesario que exista una capacidad psíquica del sujeto para comprender el hecho y su trascendencia, para ello se requiere que ese juicio lo pueda realizar quien es mayor de edad y por ello se le considere como imputable, y en el caso de que sea mayor de dieciocho años que no sufra de deficiencias mentales permanentes o transitorias"*. Por lo tanto, es importante tener en cuenta la edad del autor al evaluar la imputabilidad en casos de delitos informáticos.

Los delitos informáticos son un campo complejo que involucra la interacción de la tecnología y la conducta humana. En la evaluación de la imputabilidad del sujeto en delitos informáticos, hay varios factores técnicos y psicológicos que pueden afectar la capacidad del autor para comprender la naturaleza y consecuencias de sus acciones, así como su voluntad al cometer un delito.

Uno de los factores técnicos relevantes en la evaluación de la imputabilidad en delitos informáticos es el nivel de conocimiento técnico del autor. La tecnología informática es altamente especializada y en constante evolución, lo que significa que los autores de delitos informáticos pueden tener diferentes niveles de conocimiento técnico, algunos delincuentes informáticos pueden tener un alto grado de conocimiento técnico y comprensión de las tecnologías utilizadas, lo que podría indicar una mayor capacidad para comprender la naturaleza y las implicaciones legales de sus acciones.

Por otro lado, algunos autores de delitos informáticos pueden tener un nivel de conocimiento técnico limitado, lo que podría influir en su capacidad para comprender plenamente las consecuencias legales de sus acciones.

Además, la disponibilidad y accesibilidad de herramientas y software específico también puede afectar la imputabilidad del autor, por ejemplo, si un autor utiliza una herramienta de piratería informática o software malicioso desarrollado por terceros, podría argumentar que no comprendía plenamente la ilegalidad de sus acciones, ya que solo estaba utilizando una herramienta disponible públicamente sin tener

conocimientos técnicos avanzados, sin embargo, esto puede variar según la legislación local y las circunstancias específicas del caso.

Los factores psicológicos también pueden ser relevantes en la evaluación de la imputabilidad en delitos informáticos. Por ejemplo, la adicción a la tecnología o el trastorno del control de los impulsos pueden influir en la capacidad del autor para actuar de manera voluntaria y consciente al cometer un delito informático. La compulsión o la falta de control debido a trastornos psicológicos pueden disminuir la capacidad del autor para comprender plenamente la naturaleza y las consecuencias legales de sus acciones, lo que podría tener implicaciones en su imputabilidad.

Asimismo, otros factores psicológicos como la presión de grupo, la búsqueda de reconocimiento o la búsqueda de beneficios económicos pueden influir en la motivación del autor para cometer un delito informático, lo que a su vez puede afectar su imputabilidad, por ejemplo, un autor que comete un delito informático bajo la influencia de un grupo de amigos o con el objetivo de obtener reconocimiento social puede tener una capacidad reducida para comprender plenamente la ilegalidad de sus acciones y, por lo tanto, su imputabilidad puede verse afectada. Como señala Acosta (2020), *"los piratas realizan estos delitos como nuevos desafíos personales y para evaluar sus conocimientos frente a otros. Lo que buscan es fama y reputación a expensas de cualquier declive financiero que puedan ocasionar. La ideal del desafío es entrar en un sistema prohibido y ver hasta donde se puede llegar."*.

3.4 Conciencia sobre la antijuridicidad de la conducta

La conciencia de la antijuridicidad es un elemento importante en la evaluación de la responsabilidad penal en el contexto de la ciberdelincuencia. La ciberdelincuencia, o delitos informáticos, son acciones ilegales que se llevan a cabo utilizando tecnologías de la información y la comunicación (TIC), como computadoras, redes informáticas, internet y dispositivos electrónicos. La conciencia de la antijuridicidad se refiere a la

capacidad del autor para entender que su conducta es contraria a la ley, es decir, que está cometiendo un delito.

En el contexto de la ciberdelincuencia, la conciencia de la antijuridicidad puede presentar desafíos y reflexiones especiales debido a la naturaleza abstracta y compleja de la tecnología informática; por un lado, algunos autores de delitos informáticos pueden tener plena conciencia de la ilegalidad de sus acciones, ya que comprenden que están violando la ley al acceder, manipular o dañar sistemas informáticos o redes sin autorización. Estos autores pueden tener un conocimiento técnico avanzado y una comprensión clara de las implicaciones legales de sus acciones, lo que puede indicar una plena conciencia de la antijuridicidad de su conducta.

Sin embargo, en otros casos, la conciencia de la antijuridicidad puede ser más compleja de determinar en el contexto de la ciberdelincuencia. Esto se debe a que la tecnología informática es altamente especializada y su funcionamiento puede ser difícil de comprender para personas sin conocimientos técnicos avanzados.

Algunos autores de delitos informáticos pueden argumentar que no tenían plena conciencia de la antijuridicidad de sus acciones, ya que no comprendían completamente la ilegalidad de acceder a sistemas informáticos o redes sin autorización, o de realizar acciones como el phishing, el malware o el robo de información en línea, en este sentido, también se plantea la reflexión sobre la falta de una conciencia social generalizada sobre la antijuridicidad de ciertas conductas en el ámbito digital, algunos delincuentes informáticos pueden argumentar que su conducta no es percibida como ilegal o dañina por la sociedad en general debido a la falta de conciencia pública sobre los riesgos y consecuencias de la ciberdelincuencia. Por ejemplo, un autor que cometa un delito informático como el robo de datos o la difusión de malware puede argumentar que no tenía plena conciencia de la antijuridicidad de su conducta, ya que no era consciente de las implicaciones legales de sus acciones en el contexto digital.

Además, la rápida evolución de la tecnología informática también puede influir en la conciencia de la antijuridicidad de la conducta en el contexto de la ciberdelincuencia. Las leyes y regulaciones relacionadas con la ciberdelincuencia pueden variar de un país a otro, y lo que puede considerarse ilegal en un momento dado puede cambiar con el tiempo debido a los avances tecnológicos y a la evolución de la legislación. Esto puede plantear desafíos en la determinación de la conciencia de la antijuridicidad de la conducta en casos de ciberdelincuencia, ya que los autores pueden argumentar que no estaban plenamente conscientes de la ilegalidad de sus acciones en el momento en que las llevaron a cabo.

Aparte de los factores técnicos, también hay consideraciones psicológicas que pueden afectar la conciencia de la antijuridicidad en el contexto de la ciberdelincuencia. Por ejemplo, algunos autores de delitos informáticos pueden tener trastornos psicológicos, como adicciones tecnológicas, trastornos del control de impulsos o trastornos del espectro autista, que pueden afectar su capacidad para comprender plenamente la ilegalidad de sus acciones en el ámbito digital. Estos trastornos pueden influir en su capacidad para entender las consecuencias legales de sus acciones y pueden ser considerados como factores mitigantes en la evaluación de su conciencia de la antijuridicidad.

Por otro lado, la edad y el nivel de desarrollo emocional y cognitivo de los autores de delitos informáticos también pueden ser factores relevantes en la evaluación de su conciencia de la antijuridicidad. Los jóvenes que cometen delitos informáticos, como el ciberacoso o la difusión de imágenes íntimas sin consentimiento, pueden argumentar que no tenían plena conciencia de la ilegalidad de sus acciones debido a su falta de madurez emocional y cognitiva. En algunos casos, pueden tener una comprensión limitada de las implicaciones legales de sus acciones en línea y pueden no ser plenamente conscientes de la gravedad de sus conductas.

De la misma manera, la presión del grupo o el contexto social también puede influir en la conciencia de la antijuridicidad en el contexto de la ciberdelincuencia. Algunos

autores de delitos informáticos pueden argumentar que se vieron influenciados por sus pares o por la cultura en línea en la que participaban, lo que afectó su capacidad para comprender plenamente la ilegalidad de sus acciones. Como señala Acosta (2020), algunos ciberdelincuentes se pasan el tiempo *"tratando de destruir la reputación del compañero […] La competencia desleal de ciertos empleados y la ceguera por ser más competitivos hace que pudieran cometer un delito informático que termina perjudicando totalmente a la empresa"*. Por ejemplo, en casos de hacktivismo o acciones realizadas en nombre de una causa política o social, los autores pueden argumentar que estaban actuando en un contexto en el que la ilegalidad de sus acciones era percibida de manera diferente o justificada en función de sus creencias o valores.

3.5 Ausencia de causas excluyentes de la culpabilidad

Las causas excluyentes de culpabilidad son circunstancias o condiciones que, una vez presentes en la comisión de un delito, excluyen o eliminan la responsabilidad penal del autor, ya que se considera que no ha actuado con culpabilidad. En el contexto de los delitos informáticos, también conocidos como ciberdelitos, existen ciertas causas excluyentes de culpabilidad que pueden ser aplicables y que deben ser analizadas en la evaluación de la ausencia de culpabilidad de un autor.

Una de las causas excluyentes de culpabilidad que puede ser relevante en delitos informáticos es la legítima defensa. La legítima defensa es una situación en la cual una persona utiliza la fuerza o realiza una acción defensiva para protegerse a sí misma o a otros de un ataque ilegítimo y actual, y no incurre en responsabilidad penal, en el contexto de los delitos informáticos, un autor de un ciberdelito podría argumentar que actuó en legítima defensa para proteger sus sistemas informáticos o redes de un ataque ilegítimo, como un ataque cibernético o una intrusión no autorizada. Sin embargo, la legítima defensa en el ámbito de los delitos informáticos puede ser un tema complejo, ya que puede implicar una evaluación detallada de la proporcionalidad

y necesidad de la respuesta del autor, así como la inmediatez y legalidad del ataque que se intentaba repeler.

Otra causa excluyente de culpabilidad que puede ser aplicable en delitos informáticos es la provocación, la provocación es una situación en la cual una persona es inducida o incitada por otra a cometer un delito, y puede excluir la culpabilidad del autor debido a que su conducta se considera una respuesta razonable y comprensible ante la provocación recibida. En el contexto de los delitos informáticos, un autor de un ciberdelito podría argumentar que fue provocado por otra persona o entidad para llevar a cabo la conducta delictiva, como un ataque cibernético o una intrusión en un sistema informático, sin embargo, la provocación como causa excluyente de culpabilidad en el ámbito de los delitos informáticos puede ser evaluada con precaución, ya que puede implicar una evaluación detallada de la intencionalidad y gravedad de la provocación recibida.

Asimismo, la inexigibilidad de otra conducta también puede ser una causa excluyente de culpabilidad en delitos informáticos. La inexigibilidad de otra conducta se refiere a la situación en la cual una persona no tiene otra opción razonable y legal para actuar en determinada situación, y por lo tanto, no puede ser considerada culpable por su acción; en el contexto de los delitos informáticos, un autor de un ciberdelito podría argumentar que no tenía otra opción razonable o legal para llevar a cabo su conducta, como, por ejemplo, en situaciones de emergencia o cuando ha agotado todos los medios legales para proteger sus derechos o intereses en línea. Sin embargo, la inexigibilidad de otra conducta en el ámbito de los delitos informáticos también puede ser un tema complejo, ya que puede implicar una evaluación detallada de las circunstancias y opciones disponibles para el autor en ese momento.

En algunos casos, el error de tipo o error de prohibición también puede ser considerado como una causa excluyente de culpabilidad en delitos informáticos, el error de tipo se refiere a la situación en la cual el autor desconoce algún elemento objetivo del delito, como, por ejemplo, la naturaleza o características de la acción que está realizando.

Por otro lado, el error de prohibición se refiere a la situación en la cual el autor desconoce que su conducta es antijurídica o está prohibida por la ley. Como se señala en el sitio web Jurides (2023) *"estos tienen la capacidad de extinguir la responsabilidad penal cuando se considera probada su concurrencia. En función de la intensidad del error es posible que no se extinga la responsabilidad, pero sí que se aplique una reducción de la pena."*.

En el contexto de los delitos informáticos, un autor de un ciberdelito podría argumentar que actuó bajo un error de tipo o error de prohibición, por ejemplo, al desconocer que su conducta constituía un delito informático o al creer erróneamente que su acción era legal o permitida; sin embargo, el error de tipo o error de prohibición en el ámbito de los delitos informáticos también puede ser evaluado con cautela, ya que puede requerir una evaluación detallada de la objetividad y razonabilidad de la ignorancia del autor en relación con las normas y regulaciones informáticas.

3.6 Clases de delito informático

En el ámbito de los delitos informáticos, existen diversos tipos de conductas ilícitas que pueden ser clasificadas en diferentes categorías en función de su naturaleza, características y efectos. Como señala el sitio web Delitos Informáticos (s.f.), *"Varios organismos han propuesto diferentes clasificaciones de los delitos informáticos, aunque en general todos coinciden al enunciar como delitos informáticos los robos de identidad, fraudes y sabotajes informáticos, fugas de datos, etc."*. Por ello, algunos de los tipos de delitos informáticos más comunes incluyen el hacking, la suplantación de identidad, el robo de datos, el fraude informático, el sabotaje informático, la pornografía infantil, el grooming, la difusión no autorizada de datos privados, el phishing, el malware y el ciberterrorismo, entre otros. A continuación, se describen algunos de ellos:

- Hacking: El hacking se refiere a la intrusión no autorizada en sistemas informáticos, redes o dispositivos electrónicos con el fin de acceder, alterar, robar o

destruir información o datos. Los hackers utilizan diversas técnicas y herramientas para vulnerar la seguridad de sistemas informáticos y obtener acceso no autorizado a datos sensibles o confidenciales. Un ejemplo clásico de acceso no autorizado es el caso de Kevin Mitnick, un conocido hacker que en la década de 1980 y 1990 llevó a cabo una serie de intrusiones en sistemas informáticos de empresas y organismos gubernamentales en Estados Unidos. Mitnick utilizaba técnicas de ingeniería social y vulnerabilidades en sistemas de seguridad para obtener acceso a sistemas protegidos, robar información y causar daños. Este caso paradigmático puso de manifiesto la importancia de la protección de sistemas y la necesidad de regulaciones legales para prevenir el acceso no autorizado.

- Suplantación de identidad: La suplantación de identidad, también conocida como "phishing" o "pharming", consiste en hacerse pasar por otra persona o entidad con el fin de obtener información confidencial, como contraseñas, datos bancarios o información personal. Esto puede realizarse a través de correos electrónicos falsificados, sitios web falsos o mensajes engañosos para obtener datos sensibles de las víctimas. Un ejemplo emblemático de suplantación de identidad es el caso de Albert González, un hacker conocido como "Soupnazi" que lideró una banda criminal que robó millones de datos de tarjetas de crédito y realizó transacciones fraudulentas por varios años. González utilizó técnicas de suplantación de identidad para engañar a empresas y obtener acceso a sistemas protegidos y robar información confidencial. Este caso paradigmático puso en evidencia los riesgos y consecuencias de la suplantación de identidad en línea y la necesidad de robustas medidas de autenticación y verificación de identidad.

- Robo de datos: El robo de datos se refiere a la apropiación o copia no autorizada de información o datos electrónicos, ya sea para su uso propio o para su venta a terceros. Esto puede incluir el robo de información personal, datos comerciales, secretos comerciales, propiedad intelectual u otra información sensible almacenada en sistemas informáticos. Un ejemplo destacado de robo de datos es el caso de Equifax, una agencia de crédito de Estados Unidos que sufrió una brecha de seguridad

en 2017 que expuso los datos personales y financieros de aproximadamente 143 millones de personas. Este caso paradigmático resaltó la importancia de la protección de datos en línea, la responsabilidad de las empresas en la custodia de información sensible y las graves consecuencias del robo de datos en la privacidad y seguridad de las personas afectadas.

- Fraude informático: El fraude informático abarca una amplia gama de conductas ilícitas, como la estafa en línea, el fraude en transacciones electrónicas, la falsificación de documentos digitales, la manipulación de registros o datos electrónicos para obtener beneficios económicos o financieros ilícitos, y otras formas de fraude que involucran el uso indebido de la tecnología. Un ejemplo destacado de fraude informático es el caso de Bernard Madoff, conocido como uno de los mayores estafadores en la historia de Wall Street. Madoff utilizó un esquema Ponzi, una forma de fraude en la que los inversores más antiguos son pagados con el dinero de los inversores más nuevos, para defraudar a miles de personas y organizaciones de miles de millones de dólares. Este caso paradigmático puso de relieve la importancia de la regulación financiera y la necesidad de controles y auditorías en los sistemas financieros en línea.

- Sabotaje informático: El sabotaje informático se refiere a la destrucción, alteración o interferencia malintencionada en sistemas informáticos o redes con el fin de causar daños o perjuicios. Esto puede incluir la introducción de virus, malware o gusanos informáticos en sistemas, la realización de ataques de denegación de servicio (DDoS) para interrumpir el funcionamiento normal de una red o sitio web, o la destrucción de datos almacenados en sistemas informáticos.

- Pornografía infantil: La pornografía infantil en el ámbito informático se refiere a la creación, distribución, venta o posesión de imágenes o material que represente a menores de edad en actos sexuales o explotación sexual a través de medios electrónicos. Este tipo de delito ha llevado a numerosos casos y condenas en todo el

mundo, con implicaciones graves para las víctimas y la sociedad en general. Este caso paradigmático resalta la importancia de la cooperación internacional, la aplicación de leyes y la protección de los derechos de los niños en el ámbito digital.

- Grooming: El grooming es una forma de acoso o abuso sexual en línea que implica la manipulación y persuasión de menores de edad a través de medios electrónicos con el fin de obtener imágenes sexuales, realizar encuentros sexuales o cometer otros delitos sexuales.

- Difusión no autorizada de datos privados: La difusión no autorizada de datos privados se refiere a la divulgación o revelación no autorizada de información privada o confidencial a través de medios electrónicos, como la publicación de datos personales, financieros o sensibles en línea sin el consentimiento de la persona afectada. Esto puede incluir la divulgación de datos médicos, información financiera, detalles de tarjetas de crédito, contraseñas, entre otros.

- Malware: El malware, abreviatura de "software malicioso", se refiere a cualquier software diseñado para dañar, interferir o acceder de manera no autorizada a sistemas informáticos o dispositivos electrónicos. Esto puede incluir virus, gusanos, troyanos, ransomware, spyware y otros tipos de software malicioso que se instalan en sistemas sin el consentimiento del propietario con el fin de obtener acceso no autorizado, robar información o causar daños. Un ejemplo emblemático de malware es el gusano Stuxnet, descubierto en 2010 y considerado uno de los malware más sofisticados y destructivos de la historia. Stuxnet fue diseñado para atacar sistemas de control industrial y sabotear instalaciones nucleares en Irán. Este caso paradigmático mostró cómo el malware puede ser utilizado como una herramienta de ciberespionaje y sabotaje en conflictos geopolíticos, y resaltó la importancia de la seguridad en sistemas de infraestructura crítica.

- Ciberterrorismo: El ciberterrorismo se refiere a la realización de actos ilegales y maliciosos con fines políticos o ideológicos a través de medios electrónicos. Esto puede incluir la realización de ataques cibernéticos a infraestructuras críticas, instituciones gubernamentales o sistemas de defensa con el fin de causar daños, interrupciones o generar miedo en la sociedad.

Estos son solo algunos ejemplos de los diferentes tipos de delitos informáticos que existen en la actualidad, es importante tener en cuenta que la tecnología y el panorama de la ciberdelincuencia están en constante evolución, y nuevos tipos de delitos informáticos pueden surgir con el avance de la tecnología y las cambiantes dinámicas del ciberespacio.

3.7 Análisis sobre las legislaciones en México comparado con otros países sobre el delito informático

La legislación en materia de delitos informáticos varía de un país a otro, ya que está influenciada por diversos factores, como la cultura, la historia, el nivel de desarrollo tecnológico y las necesidades específicas de cada jurisdicción. En el caso de México, la legislación sobre delitos informáticos ha evolucionado en los últimos años para adaptarse a los avances tecnológicos y las cambiantes formas de ciberdelincuencia.

En México, la legislación en materia de delitos informáticos está principalmente contenida en Codigo Penal Federal en su capítulo II "Acceso ilícito a sistemas y equipos de informática". Esta ley establece un marco legal para la prevención, investigación, persecución y sanción de delitos informáticos en México, y abarca una amplia gama de actividades ilícitas en el ámbito digital, incluyendo acceso ilícito a sistemas y datos, daño a sistemas informáticos, sabotaje informático, fraude electrónico, pornografía infantil, entre otros.

En comparación con otros países, la legislación mexicana en materia de delitos informáticos es considerada relativamente moderna y completa, ya que aborda

diversos aspectos de la ciberdelincuencia y establece penas y sanciones proporcionales a la gravedad de los delitos. Sin embargo, algunos expertos han señalado que aún existen áreas de mejora en la legislación mexicana, como la clarificación de algunos conceptos, la armonización con tratados internacionales y la adaptación a las nuevas formas de ciberdelincuencia que van surgiendo con la evolución tecnológica.

La legislación en materia de delitos informáticos varía ampliamente en diferentes países alrededor del mundo. Algunos países tienen leyes específicas sobre delitos informáticos, mientras que otros incorporan disposiciones relacionadas con la ciberdelincuencia en sus leyes penales generales o en otras legislaciones especializadas. Algunos países que han desarrollado legislaciones avanzadas en materia de delitos informáticos incluyen Estados Unidos, Canadá, Reino Unido, Australia, Singapur, Japón, Brasil y Sudáfrica, entre otros.

En general, la legislación en estos países tiende a ser amplia y abarcar una amplia gama de delitos informáticos, con enfoques similares en la protección de la confidencialidad, integridad y disponibilidad de datos, la prevención y sanción de accesos no autorizados, la protección de la propiedad intelectual y la privacidad, y la cooperación internacional en la lucha contra la ciberdelincuencia. Sin embargo, también existen diferencias significativas en las leyes y regulaciones específicas de cada país, como los tipos de delitos informáticos tipificados, las penas y sanciones establecidas, los procedimientos de investigación y enjuiciamiento, y los mecanismos de cooperación internacional.

Un aspecto importante a tener en cuenta en la comparación de la legislación en materia de delitos informáticos es la velocidad de cambio y evolución tecnológica, que puede superar la capacidad de adaptación de las leyes y regulaciones existentes, aa ciberdelincuencia es una realidad en constante evolución, con nuevas formas de ataques y amenazas que surgen constantemente en el panorama digital. Por lo tanto, las legislaciones en materia de delitos informáticos en todo el mundo enfrentan el

desafío de mantenerse actualizadas y adaptarse a los avances tecnológicos y a las cambiantes tácticas de los ciberdelincuentes.

En el caso de México, si bien la legislación en materia de delitos informáticos es considerada moderna y completa, existen algunos desafíos y áreas de mejora. Por ejemplo, se ha señalado la necesidad de una mayor clarificación de algunos conceptos en la ley, como la definición precisa de algunos delitos informáticos y la especificación de las conductas que constituyen acceso ilícito a sistemas y datos, daño a sistemas informáticos, sabotaje informático, y otros delitos cibernéticos.

También se ha destacado la importancia de armonizar la legislación mexicana con tratados internacionales y convenios en materia de ciberdelincuencia, con el fin de mejorar la cooperación internacional en la lucha contra la ciberdelincuencia transnacional.

En comparación con otros países, algunos desafíos que enfrenta la legislación mexicana en materia de delitos informáticos incluyen la necesidad de fortalecer los mecanismos de prevención, detección e investigación de la ciberdelincuencia, así como mejorar la capacidad técnica y forense de las autoridades encargadas de la aplicación de la ley en el ámbito digital. Además, la celeridad en la evolución tecnológica y la aparición constante de nuevas formas de ciberdelincuencia requiere que la legislación se actualice de manera constante para adaptarse a los cambios en el panorama digital y asegurar una respuesta efectiva a los delitos informáticos.

En términos de cooperación internacional, México ha establecido acuerdos bilaterales y multilaterales con otros países para la prevención, investigación y persecución de delitos informáticos transnacionales, por ejemplo, la Unidad Especializada en Delitos Fiscales y Financieros (UEIDFF), la cual *“Es la Unidad encargada de investigar y perseguir delitos fiscales y financieros que requieran de atención especializada, con estricto apego a los principios de certeza, legalidad, objetividad, imparcialidad y profesionalismo.”* (Gobierno de México, s.f.).

Sin embargo, aún existen desafíos en la cooperación internacional en el ámbito de la ciberdelincuencia, como la identificación y extradición de ciberdelincuentes que operan en jurisdicciones extranjeras, la obtención de pruebas digitales y la coordinación de esfuerzos en la persecución de delitos informáticos a nivel global; así pues, la ciberdelincuencia es un fenómeno transnacional que no conoce fronteras y que se ha convertido en una amenaza global en la era digital.

Los ciberdelincuentes pueden operar desde cualquier parte del mundo y llevar a cabo actividades delictivas que trascienden las jurisdicciones nacionales. Por lo tanto, la armonización y cooperación internacional en la lucha contra la ciberdelincuencia se ha vuelto esencial para abordar este desafío de manera efectiva.

En el caso específico de México, como en muchos otros países, la naturaleza transnacional de la ciberdelincuencia plantea desafíos significativos en la persecución y prevención de los delitos informáticos. Los ciberdelincuentes pueden utilizar redes internacionales para llevar a cabo actividades ilícitas, como ataques cibernéticos, fraude electrónico, robo de datos y otros delitos informáticos, lo que hace que sea difícil para un solo país enfrentar eficazmente estos delitos.

La armonización de la legislación en materia de delitos informáticos entre países es esencial para asegurar que no haya lagunas legales o brechas que los ciberdelincuentes puedan explotar. La falta de armonización puede permitir que los ciberdelincuentes evadan la persecución legal mediante la explotación de diferencias en las leyes y regulaciones de diferentes países.

Por lo tanto, es crucial que los países establezcan mecanismos de cooperación y coordinación para alinear sus legislaciones en materia de ciberdelincuencia y asegurar que los delincuentes no encuentren refugio en jurisdicciones que tengan leyes menos rigurosas o inadecuadas en este ámbito.

A modo de complemento, a continuación se presenta una tabla que contiene la cantidad de delitos informáticos tipificados por país en Latinoamérica en el año 2016.

Figura 2. Delitos informáticos tipificados por país.

Puesto	País	Cantidad
1.º	República Dominicana	31
2.º	Paraguay	22
3.º	Costa Rica	21
4.º	México	20
5.º	Venezuela	20
6.º	Ecuador	19
7.º	Chile	14

Fuente: Redalyc (2016).

3.8 Análisis sobre ejemplos en México de delito informático

En México, al igual que en otros países, se han registrado numerosos casos de delitos informáticos que han afectado a individuos, empresas y entidades gubernamentales. Estos casos han sido investigados y procesados por las autoridades mexicanas, y proporcionan ejemplos concretos de la naturaleza y el alcance de la ciberdelincuencia en el país.

Un ejemplo de delito informático en México es el fraude electrónico. Se han registrado casos de phishing, donde los ciberdelincuentes envían correos electrónicos falsificados o mensajes de texto para obtener información confidencial, como contraseñas o datos bancarios, de personas desprevenidas. Estos datos son luego utilizados para cometer fraudes, como el robo de identidad o la realización de transacciones fraudulentas en línea, según un artículo de Bussiness Insider, la presión de fraude en el comercio electrónico en México alcanzó un nivel 220% mayor que a la época antes de la pandemia (Cueto, 2022); otro ejemplo es el ransomware, que es un tipo de malware que cifra los archivos de una computadora o sistema informático y

exige un rescate para desbloquearlos; ha habido casos en México donde empresas y organizaciones han sido víctimas de ataques de ransomware, lo que ha provocado la paralización de sus operaciones y pérdidas económicas significativas, según un artículo de El Economista, Foxconn, una empresa de productos electrónicos que es proveedora de Apple, ha sufrido recientemente al menos dos ciberataques de ransomware en México (Riquelme, 2022).

También se han registrado casos de intrusión informática, donde los ciberdelincuentes acceden de manera no autorizada a sistemas informáticos o redes, con el objetivo de robar información sensible o causar daños. Estos casos pueden involucrar a individuos, empresas o entidades gubernamentales, y han resultado en la exposición de datos confidenciales y la interrupción de servicios. Un ejemplo de esto es el malware Fallchill, el cual *"fue detectado en varios equipos de una empresa de telecomunicaciones en la Ciudad de México."* (Orca, s.f.), el cual era capaz de intervenir los archivos, modificar los procesos y extraer información, así como borrarse a sí mismo para evitar ser detectado.

La suplantación de identidad en línea también es un delito informático que ha sido reportado en México, los ciberdelincuentes crean perfiles falsos en redes sociales, sitios web o correos electrónicos para obtener información personal o cometer fraudes en nombre de otra persona, esto puede tener consecuencias graves para las víctimas, como la pérdida de reputación, el robo de identidad o el acoso en línea. Según datos de El Economista, *"a escala mundial, México ocupa el octavo lugar en suplantación de identidad."* (Badillo, 2022), además, se han registrado casos de pornografía infantil en línea en México, que es un delito grave que involucra la producción, distribución o posesión de material pornográfico que involucra a menores de edad. Las autoridades mexicanas han llevado a cabo operativos para combatir este tipo de delito informático, identificar a los responsables y proteger a los menores afectados; de hecho, según un informe de Infobae (2023), *"En septiembre del año 2022 un hombre y una mujer fueron detenidos por presuntamente producir pornografía infantil bajo la fachada de dar clases de regularización a menores de edad en la Ciudad de México."*

Por lo tanto, los delitos informáticos en México tienen implicaciones jurídicas, sociales y económicas significativas. Los impactos en las víctimas, en las empresas y en la sociedad en general son diversos y abarcan desde pérdidas financieras hasta consecuencias emocionales y psicológicas, la prevención, detección y persecución de los delitos informáticos son desafíos importantes que requieren una legislación robusta, cooperación internacional, concientización y educación en ciberseguridad, así como una respuesta eficaz por parte de las autoridades para proteger a las víctimas y salvaguardar la integridad de los sistemas informáticos.

3.9 Derecho comparado caso específico (México-Venezuela) sobre delito informático

El análisis comparativo de la legislación y jurisprudencia en materia de delitos informáticos en México y Venezuela revela similitudes y diferencias en la manera en que ambos países abordan este tipo de delitos en su marco legal.

En primer lugar, en México, los delitos informáticos están contemplados en Código Penal Federal en su Capítulo II “Acceso ilícito a sistemas y equipos de informática”, adicionado mediante decreto publicado en el Diario oficial en fecha 17/05/1999 , la cual fue creada con el objetivo de tipificar y sancionar conductas ilícitas en el uso de las tecnologías de la información y comunicación, esta ley establece diversos tipos de delitos informáticos, como acceso ilícito a sistemas y equipos de informática, sabotaje informático, fraude informático, entre otros; además, prevé sanciones que van desde multas hasta penas privativas de libertad, dependiendo de la gravedad del delito cometido; todo esto se dio a conocer en la legislación punitiva de 1999 (UNAM, s.f.).

Por otro lado, en Venezuela, los delitos informáticos son regulados principalmente por la Ley Especial Contra los Delitos Informáticos (2001), aprobada en el año 2001, la cual busca proteger la seguridad de la información y los sistemas informáticos en el país. Esta ley establece diversas conductas delictivas, como acceso indebido a sistemas informáticos, sabotaje informático, daño a la propiedad intelectual, entre otros,

también establece sanciones que incluyen multas y penas privativas de libertad, de acuerdo a la gravedad del delito cometido.

En términos de jurisprudencia, ambos países han desarrollado una serie de precedentes judiciales en casos de delitos informáticos, por ejemplo, en México, la Suprema Corte de Justicia de la Nación ha emitido resoluciones en casos de acceso ilícito a sistemas informáticos, estableciendo criterios sobre la tipificación y sanción de este delito, asimismo, en Venezuela, el Tribunal Supremo de Justicia ha emitido fallos en casos de sabotaje informático y acceso indebido a sistemas informáticos, interpretando y aplicando la legislación vigente en la materia; sin embargo, en Venezuela, la Ley Especial Contra los Delitos Informáticos establece la figura del "sabotaje informático", que no está contemplada en la legislación mexicana.

En cuanto a las sanciones, también existen diferencias. Por ejemplo, en México, las penas privativas de libertad por delitos informáticos pueden ser de hasta 20 años, mientras que, en Venezuela, las penas máximas son de hasta 10 años de prisión, además, en México, la ley contempla la posibilidad de aplicar medidas cautelares como la suspensión del acceso a internet o la restricción del uso de tecnologías de la información, mientras que, en Venezuela, no se contemplan estas medidas en la legislación.

La lucha contra la ciberdelincuencia en México y Venezuela ha enfrentado diversos desafíos, pero también ha generado lecciones aprendidas y mejores prácticas que pueden servir como referencia para otros países y oportunidades de cooperación y armonización normativa en la materia.

Una de las principales lecciones aprendidas en la lucha contra la ciberdelincuencia en ambos países es la importancia de contar con una legislación actualizada y robusta que tipifique claramente los delitos informáticos y establezca sanciones proporcionadas y efectivas, tanto México como Venezuela han desarrollado leyes específicas que buscan hacer frente a los retos de la ciberdelincuencia, y estas

legislaciones han sido actualizadas en respuesta a la evolución constante de las tecnologías de la información y comunicación, es importante destacar que la actualización periódica de la legislación es fundamental para mantenerla actualizada y adaptada a las nuevas formas de ciberdelitos que van surgiendo.

Otra lección aprendida es la necesidad de fortalecer los mecanismos de cooperación y coordinación entre las autoridades nacionales e internacionales en la lucha contra la ciberdelincuencia. Los delitos informáticos tienen un carácter transnacional, lo cual dificulta su investigación y persecución, por ello, la cooperación internacional y el intercambio de información entre países son elementos clave en la lucha contra la ciberdelincuencia, México y Venezuela han establecido acuerdos bilaterales y participan en organismos internacionales para fortalecer la cooperación en esta materia, lo cual puede servir como ejemplo para otros países, además, se ha evidenciado la importancia de la capacitación y especialización de los operadores de justicia en el combate a la ciberdelincuencia. Los delitos informáticos requieren de un conocimiento técnico especializado para su investigación y persecución, por lo que es fundamental contar con fiscales, jueces, policías y otros profesionales del derecho debidamente capacitados en esta área, en este sentido, tanto México como Venezuela han implementado programas de capacitación y formación en ciberseguridad y delitos informáticos para su personal de justicia, lo cual representa una buena práctica a seguir.

En términos de oportunidades de cooperación y armonización normativa, México y Venezuela podrían explorar la posibilidad de establecer acuerdos bilaterales o multilaterales para fortalecer la colaboración en la lucha contra la ciberdelincuencia, esto podría incluir el intercambio de información, experiencias y buenas prácticas, así como la cooperación en investigaciones y en la persecución de los delitos informáticos que involucren a ambos países.

3.10 Las nuevas técnicas y la clasificación *iter criminis* y delito

En los últimos años, se ha observado un rápido avance en las tecnologías de la información y la comunicación, lo cual ha llevado a la aparición de nuevas técnicas utilizadas en la comisión de delitos informáticos, estas técnicas, conocidas como ciberataques, han evolucionado en complejidad y sofisticación, lo que representa un desafío para las legislaciones y los sistemas de justicia en todo el mundo.

Una de las técnicas más utilizadas en la comisión de delitos informáticos es el phishing, el cual, como ya se mencionó anteriormente, consiste en engañar a una persona para obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales, mediante la suplantación de identidad.

Otra técnica utilizada en la comisión de delitos informáticos es el ransomware, que, como ya se dijo, consiste en el secuestro de los datos de una computadora o sistema informático, exigiendo un rescate para su liberación, el ransomware se propaga a través de archivos adjuntos de correo electrónico, enlaces maliciosos, descargas de software no confiable o aprovechando vulnerabilidades en sistemas operativos o software. Una vez que el ransomware infecta un sistema, encripta los datos y muestra un mensaje de rescate solicitando el pago en criptomonedas u otra forma de pago para liberar los datos.

El cryptojacking es otra técnica utilizada en la comisión de delitos informáticos, que consiste en utilizar el poder de procesamiento de una computadora o dispositivo sin el consentimiento del propietario para minar criptomonedas, los ciberdelincuentes infectan los sistemas con malware que realiza la minería de criptomonedas de forma encubierta, utilizando los recursos de la computadora de la víctima para obtener beneficios económicos ilegales, además, también se han observado nuevas técnicas como el spoofing, que implica falsificar la dirección de origen de un correo electrónico o mensaje para hacerlo parecer legítimo, el pharming, que redirige a los usuarios a sitios web falsificados para obtener su información confidencial, y el malware de

acceso remoto (RAT, por sus siglas en inglés), que permite a los ciberdelincuentes controlar de forma remota una computadora o dispositivo para realizar acciones ilegales.

La clasificación de estos delitos informáticos se realiza a través del concepto de iter criminis, que hace referencia a las diferentes etapas de la comisión del delito. En el caso de las nuevas técnicas utilizadas en la comisión de delitos informáticos, el iter criminis suele involucrar las siguientes etapas:

- Fase de preparación: Los ciberdelincuentes investigan y planifican el ataque, identificando vulnerabilidades en sistemas informáticos, creando malware, estableciendo infraestructuras y buscando posibles víctimas.

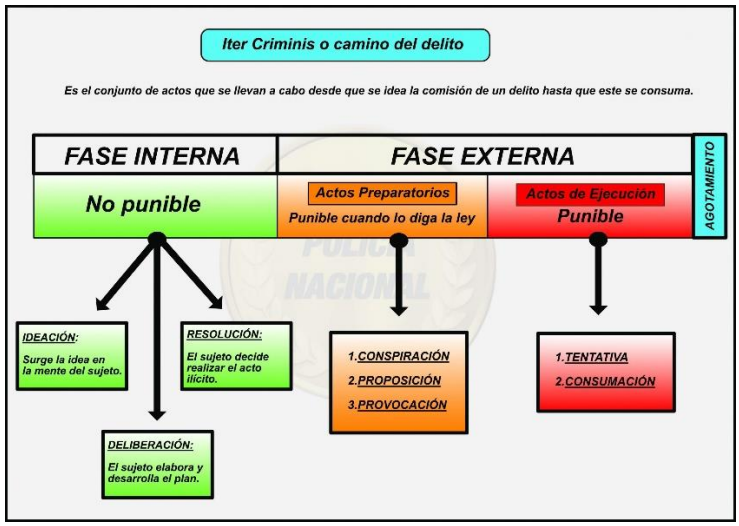
- Fase de ejecución: Los ciberdelincuentes llevan a cabo el ataque utilizando las técnicas mencionadas anteriormente, como el phishing, ransomware, cryptojacking, entre otros. Realizan el envío de correos electrónicos falsificados, infectan sistemas con malware, secuestran datos o utilizan el poder de procesamiento de las computadoras de las víctimas para minar criptomonedas.

- Fase de ocultamiento: Una vez que han realizado el ataque, los ciberdelincuentes buscan encubrir sus huellas, borrando evidencia, ocultando la ruta de acceso y limpiando su presencia en los sistemas afectados para evitar ser rastreados.

- Fase de beneficio: En esta etapa, los ciberdelincuentes buscan obtener beneficios económicos ilegales, como el rescate exigido en el caso de ransomware, la venta de información confidencial obtenida a través de phishing, o las ganancias generadas por la minería de criptomonedas en el caso de cryptojacking.

Es importante destacar que estas nuevas técnicas utilizadas en la comisión de delitos informáticos presentan un desafío para la legislación y la aplicación de la justicia, ya que se requiere de una constante actualización y adaptación de las leyes y los sistemas de justicia para enfrentar estos nuevos desafíos tecnológicos.

Figura 3. Explicación gráfica sobre Iter Criminis.



Fuente: Sicol Policía Nacional (2022).

CAPÍTULO IV. REGULACIÓN Y PREVENCIÓN DEL CIBERDELITO EN MÉXICO

4. Tratados internacionales sobre el delito informático

La Convención sobre Cibercrimen del Consejo de Europa, también conocida como el Convenio de Budapest, es uno de los tratados internacionales más relevantes en el ámbito de la regulación y prevención del ciberdelito, adoptada en 2001 y en vigor desde 2004, esta convención tiene como objetivo principal armonizar las legislaciones y fortalecer la cooperación internacional en la lucha contra el ciberdelito, incluyendo delitos informáticos, delitos relacionados con la tecnología de la información y delitos contra la propiedad intelectual. Según un artículo de la Biblioteca del Congreso Nacional de Chile, *"El tratado ha sido ratificado por 60 Estados, incluidos los Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia y Japón."*

En el contexto de México, la adopción y aplicación de la Convención sobre Cibercrimen del Consejo de Europa ha sido un tema de gran relevancia en los últimos años. México es uno de los países firmantes de este convenio, lo cual implica un compromiso para implementar las medidas y políticas establecidas en él, así como armonizar su legislación interna con los principios y normas contenidos en dicho tratado.

El análisis de la adopción y aplicación de la Convención sobre Cibercrimen del Consejo de Europa en México implica evaluar cómo se ha implementado en la legislación y práctica mexicana, así como identificar los retos y oportunidades que ha enfrentado el país en su proceso de armonización y cumplimiento de dicho convenio.
Es importante destacar que México ha realizado esfuerzos significativos en la regulación y prevención del ciberdelito, y la adopción de la Convención sobre Cibercrimen del Consejo de Europa ha sido un paso importante en esta dirección.

Uno de los aspectos a analizar es la incorporación de los principios y normas establecidos en la Convención en la legislación mexicana, esto incluye la revisión de las leyes y regulaciones existentes en México para determinar su compatibilidad con

los estándares internacionales establecidos en el Convenio de Budapest; asimismo, se debe evaluar la existencia de lagunas o áreas de mejora en la legislación mexicana en lo que respecta a la regulación y prevención del ciberdelito, y proponer posibles modificaciones o actualizaciones necesarias para garantizar la armonización con la Convención.

Otro aspecto importante a analizar es la implementación de políticas y medidas de prevención del ciberdelito en México, en concordancia con los principios y directrices establecidos en el Convenio de Budapest, esto implica evaluar la efectividad de las políticas y programas existentes en México para prevenir y combatir el ciberdelito, así como identificar posibles áreas de mejora y proponer estrategias innovadoras y eficientes para la prevención del ciberdelito en el país.

En el marco de la regulación y prevención del ciberdelito en México, los tratados bilaterales y multilaterales de cooperación internacional desempeñan un papel relevante, estos tratados son acuerdos entre países que buscan fortalecer la colaboración en la lucha contra el ciberdelito, mediante el intercambio de información, la asistencia legal mutua y la cooperación operativa en investigaciones y enjuiciamientos de delitos informáticos.

En el contexto de México, estos tratados internacionales han sido de gran importancia para fortalecer su capacidad para combatir el ciberdelito, así como para prevenir y sancionar eficazmente a los delincuentes cibernéticos que operan a nivel transnacional; algunos de los tratados bilaterales y multilaterales de cooperación en la lucha contra el ciberdelito que son relevantes en el contexto de México incluyen:

- Tratados bilaterales con otros países: México ha establecido tratados bilaterales con varios países, con el objetivo de fortalecer la cooperación en la lucha contra el ciberdelito, estos tratados incluyen acuerdos de asistencia legal mutua, que permiten el intercambio de información y pruebas electrónicas en casos de delitos informáticos, así como la colaboración en investigaciones y enjuiciamientos de ciberdelincuentes.

Estos acuerdos bilaterales también pueden establecer mecanismos de cooperación operativa, como equipos conjuntos de investigación o patrullas cibernéticas, que buscan prevenir y combatir el ciberdelito de manera coordinada. Algunos de estos tratados son: Tratado de Asistencia Jurídica Mutua en Materia Penal entre México y Estados Unidos, Acuerdo de Cooperación en Materia de Seguridad entre México y Canadá, Acuerdo de Cooperación en Materia de Seguridad entre México y España (Pérez, S. A. R., 2021).

- Tratados multilaterales: México también ha participado en tratados multilaterales, como la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional y su Protocolo Adicional relativo a la Lucha contra el Ciberdelito (United Nations Office on Drugs and Crime, s.f.). Estos tratados internacionales buscan establecer un marco normativo y una plataforma de cooperación internacional para prevenir y combatir el ciberdelito a nivel global. México ha ratificado estos tratados y ha adoptado medidas para implementar sus disposiciones en su legislación interna, con el objetivo de fortalecer su capacidad para enfrentar el ciberdelito en colaboración con otros países.

- Acuerdos de cooperación regional: México también ha participado en acuerdos de cooperación regional, como la Estrategia de Seguridad de Centroamérica (ESCA) (Secretaría De Relaciones Exteriores, s. f.), que busca fortalecer la cooperación en la lucha contra el ciberdelito en la región de América Central. Estos acuerdos buscan establecer mecanismos de colaboración regional, intercambio de información y capacitación para prevenir y enfrentar el ciberdelito en conjunto con otros países de la región.

La relevancia de estos tratados bilaterales y multilaterales de cooperación en el contexto de México radica en la posibilidad de fortalecer su capacidad para enfrentar el ciberdelito de manera efectiva y en colaboración con otros países, estos acuerdos permiten el intercambio de información clave en investigaciones de delitos informáticos, la asistencia legal mutua para obtener pruebas electrónicas en el

extranjero y la coordinación operativa en la identificación y persecución de ciberdelincuentes que operan a nivel internacional.

El análisis comparativo de la legislación internacional sobre delitos informáticos y su relación con la regulación en México es un tema relevante en el contexto de la regulación y prevención del ciberdelito en el país. La evolución y armonización de las leyes y regulaciones internacionales en el ámbito de los delitos informáticos han generado un marco legal que busca abordar los desafíos y complejidades de la ciberdelincuencia a nivel global. México, como país miembro de la comunidad internacional, ha adoptado y ratificado varios tratados internacionales sobre delitos informáticos con el objetivo de armonizar su legislación nacional con los estándares internacionales y fortalecer su marco legal en la lucha contra el ciberdelito.

Asimismo, es importante destacar que la Convención de Budapest sobre Cibercrimen establece disposiciones para la obtención de pruebas electrónicas, la preservación de la evidencia digital, la protección de los derechos de privacidad y la cooperación transfronteriza en la obtención y transferencia de pruebas electrónicas.

En el caso de México, se ha avanzado en la adopción de regulaciones y legislación en línea con los estándares internacionales establecidos por la Convención de Budapest. Por ejemplo, en 2019 se reformó el Código Penal Federal (Código Penal Federal, 2020) y se incorporaron disposiciones relacionadas con los delitos informáticos, estableciendo sanciones para la obtención ilegal de datos, acceso no autorizado a sistemas informáticos, daño a sistemas informáticos, sabotaje informático, entre otros; Además se establecieron procedimientos para la obtención de pruebas electrónicas y la preservación de la evidencia digital en línea con los principios de la Convención de Budapest.

Sin embargo, a pesar de los avances en la legislación mexicana, existen algunos desafíos y áreas de mejora en la regulación y prevención del ciberdelito en el país, por ejemplo, la legislación mexicana aún enfrenta retos en términos de la actualización

constante de las normas y regulaciones para hacer frente a la evolución rápida de la tecnología y las nuevas formas de ciberdelincuencia, además, es necesario fortalecer los mecanismos de cooperación internacional en la investigación y persecución de delitos informáticos, en línea con los principios de la Convención de Budapest.

Es importante mencionar que México también ha suscrito otros tratados internacionales relevantes en el ámbito de la ciberseguridad, como el Convenio de Budapest del Grupo de Estados contra la Corrupción (GRECO) (Consejo de Europa, 2001) y la Convención Interamericana contra la Corrupción de la Organización de los Estados Americanos (OEA) (Organización de los Estados Americanos, 1996). Estos tratados buscan fortalecer la cooperación internacional en la prevención y combate de la corrupción, incluyendo la corrupción en el ámbito digital.

En el contexto de la regulación y prevención del ciberdelito en México, es importante mencionar también la Ley Federal de Telecomunicaciones y Radiodifusión (Cámara de Diputados del H. Congreso de la Unión, 2021), que establece disposiciones relacionadas con la seguridad de las redes y sistemas de información en el país, esta ley busca promover la protección de la infraestructura crítica de telecomunicaciones y radiodifusión, así como establecer medidas para la prevención y respuesta ante incidentes de seguridad cibernética.

En el ámbito de la prevención del ciberdelito, México ha implementado diversas iniciativas y programas, tanto a nivel gubernamental como a nivel de la sociedad civil y el sector privado. Por ejemplo, la Guardia Nacional tiene a su cargo diversas: Unidades de Policía Cibernética, que se articulan como parte del Sistema Nacional de Seguridad Pública, así como programas de concientización y educación sobre seguridad cibernética en colaboración con el sector privado y organizaciones de la sociedad civil.

La armonización de la legislación nacional con los tratados internacionales sobre ciberdelito es un desafío y una oportunidad para los países, incluyendo México, que

buscan fortalecer su marco legal y prevención del ciberdelito. Según un artículo de Amnesty International, el Ministerio de Asuntos Exteriores define tratado internacional como *"un acuerdo celebrado por escrito entre Estados, o entre Estados y otros sujetos de derecho internacional, como las organizaciones internacionales, y regido por el Derecho Internacional"* (Amnesty International, s.f.). Los tratados internacionales establecen estándares y principios que buscan promover la cooperación transnacional en la lucha contra el ciberdelito y garantizar la protección de los derechos de las víctimas y la seguridad en línea, sin embargo, la armonización de la legislación nacional con estos tratados implica enfrentar una serie de retos y aprovechar oportunidades para lograr una regulación efectiva y coherente en este ámbito.

Uno de los principales retos en la armonización de la legislación nacional con los tratados internacionales sobre ciberdelito es la rapidez con la que evoluciona la tecnología y las nuevas formas de ciberdelincuencia, los ciberdelincuentes utilizan constantemente nuevas herramientas y técnicas para llevar a cabo actividades ilegales en línea, lo que requiere una respuesta legislativa y reguladora ágil y actualizada, la legislación nacional debe ser lo suficientemente flexible para adaptarse a estos cambios y garantizar la efectiva persecución y sanción de los delitos informáticos.

Otro reto importante es la falta de consenso y uniformidad en la interpretación y aplicación de los tratados internacionales sobre ciberdelito; cada país tiene su propio sistema legal y procesos judiciales, lo que puede generar diferencias en la interpretación y aplicación de las disposiciones de los tratados internacionales, esto puede dificultar la cooperación transnacional en la obtención de pruebas y la persecución de los delitos informáticos, es necesario asegurar una interpretación y aplicación coherente de los tratados internacionales en la legislación nacional, a fin de facilitar la cooperación internacional y la armonización de los marcos legales.

La complejidad y la transnacionalidad de los delitos informáticos también presentan retos en la armonización de la legislación nacional con los tratados internacionales, los ciberdelincuentes pueden operar desde cualquier parte del mundo, utilizando

servidores y redes ubicadas en diferentes jurisdicciones, esto dificulta la persecución y sanción de los delitos informáticos, ya que los procedimientos legales pueden variar de un país a otro; es necesario establecer mecanismos de cooperación internacional efectivos, en línea con los principios de los tratados internacionales, para garantizar la persecución efectiva de los ciberdelincuentes, así como la obtención y transferencia de pruebas electrónicas.

4.1 México y la regulación de delitos cibernéticos

México, al igual que muchos otros países en el mundo, ha enfrentado el desafío de regular y prevenir los delitos cibernéticos en un contexto de creciente digitalización y dependencia de la tecnología, la regulación de los delitos cibernéticos en México se ha ido desarrollando en los últimos años con el objetivo de proteger a los ciudadanos, las empresas y el gobierno contra los riesgos y amenazas en línea, así como promover el uso seguro y responsable de la tecnología.

En México, la regulación de los delitos cibernéticos se encuentra principalmente en el Código Penal Federal, en el capítulo II "Acceso ilícito a sistemas y equipos de informática", publicado en el Diario Oficial de la Federación de fecha: 17-05-1999. Este capítulo tiene como objetivo establecer las normas y los procedimientos para prevenir, sancionar y erradicar los delitos informáticos en México, así como promover la confianza en el uso de las tecnologías de la información.

La regulación de los delitos cibernéticos en México también contempla medidas de prevención, como la promoción de la ciberseguridad, la protección de datos personales, la identificación y notificación de incidentes cibernéticos, la implementación de medidas de seguridad en sistemas y redes informáticas, y la promoción de la concientización y educación en seguridad cibernética.

La cooperación internacional en la prevención y persecución del ciberdelito es esencial, dado que los ciberdelincuentes operan a nivel global y los efectos de los

delitos cibernéticos pueden trascender fronteras. México ha buscado fortalecer su colaboración con otros países en la lucha contra el ciberdelito, incluyendo la participación en iniciativas internacionales de cooperación y el intercambio de información y mejores prácticas en seguridad cibernética.

Sin embargo, a pesar de los avances en la regulación del ciberdelito en México, aún existen retos y desafíos importantes que enfrenta el país en este ámbito, uno de ellos es la capacidad de investigación y persecución de los delitos cibernéticos, debido a la constante evolución de las tecnologías y la sofisticación de los ataques cibernéticos. La capacitación y especialización de los cuerpos de seguridad y de justicia en materia de ciberdelito, así como la inversión en infraestructura y herramientas tecnológicas adecuadas, son aspectos que requieren atención continua para mejorar la efectividad en la prevención, investigación y persecución de estos delitos.

A pesar de los retos, México también cuenta con oportunidades en la armonización de la legislación nacional con los tratados internacionales sobre ciberdelito, la adopción de estándares y mejores prácticas internacionales en la regulación del ciberdelito puede contribuir a fortalecer la legislación nacional y asegurar que se encuentre a la vanguardia en la protección de los ciudadanos, empresas y gobierno contra las amenazas cibernéticas; la cooperación internacional también puede ser una oportunidad para el intercambio de conocimientos y experiencias en la lucha contra el ciberdelito, así como la identificación de áreas de mejora y oportunidades de colaboración para fortalecer las capacidades en el combate a los delitos cibernéticos.

El marco jurídico actual de la regulación del ciberdelito en México está conformado por diversas normas y regulaciones que buscan prevenir, investigar y sancionar los delitos cometidos a través de medios electrónicos, estas normas se han ido actualizando a lo largo del tiempo para adaptarse a los cambios tecnológicos y a las nuevas formas de delincuencia cibernética.

La Ley Federal de Telecomunicaciones y Radiodifusión también juega un papel importante en la regulación del ciberdelito en México, ya que establece las obligaciones de los concesionarios y usuarios de telecomunicaciones en materia de seguridad de la red y protección de la información, esta ley establece medidas para garantizar la confidencialidad, integridad y disponibilidad de la información en redes de telecomunicaciones, así como la prevención y sanción de los delitos cometidos a través de estos medios.

En el ámbito administrativo, diversas dependencias del gobierno mexicano, como la Fiscalía General de la República (FGR), la Secretaría de Seguridad y Protección Ciudadana (SSPC), el Centro Nacional de Inteligencia (CNI) y la Comisión Nacional de Seguridad (CNS), entre otras, también cuentan con facultades y responsabilidades en la prevención y combate del ciberdelito, estas dependencias trabajan en coordinación para investigar y sancionar los delitos cibernéticos, así como para implementar políticas de prevención, capacitación y concientización en materia de ciberseguridad.

Por todo lo anterior, se puede decir que la regulación del ciberdelito en México ha experimentado avances significativos en los últimos años, sin embargo, también enfrenta desafíos importantes que afectan su eficacia en la prevención, persecución y sanción de los delitos cibernéticos; a continuación se mencionan resumidamente los avances y desafíos en la regulación del ciberdelito en México.
Avances en la regulación del ciberdelito en México:

Marco jurídico: México cuenta con un marco jurídico específico para la regulación del ciberdelito, que incluye diversas leyes y regulaciones, como la Ley Federal de Telecomunicaciones y Radiodifusión, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la Ley Federal del Derecho de Autor, y el Código Penal Federal, entre otras. Estas normativas establecen los delitos cibernéticos y las sanciones correspondientes, así como los procedimientos para la investigación, persecución y sanción de los mismos.

- Creación de instituciones especializadas: Se ha avanzado en la creación de instituciones especializadas encargadas de la prevención, investigación y persecución del ciberdelito en México. La Guardia Nacional tiene a su cargo diversas: Unidades de Policía Cibernética, que se articulan como parte del Sistema Nacional de Seguridad Pública; asi como la Secretaria de Seguridad Ciudadana de la Ciudad de México, tiene a su cargo una Policía Cibernética; son algunas de las instituciones encargadas de la atención de los delitos cibernéticos en el país. Estas instituciones han desarrollado capacidades técnicas y tecnológicas especializadas para hacer frente a los retos del ciberdelito.

- Cooperación internacional: México ha fortalecido la cooperación internacional en la lucha contra el ciberdelito, estableciendo acuerdos y convenios con otros países y organismos internacionales. Esto ha permitido la obtención de apoyo técnico y tecnológico, así como la colaboración en la investigación y persecución de delitos cibernéticos transnacionales. La cooperación internacional es crucial debido a la naturaleza global del ciberdelito, que trasciende las fronteras y requiere una respuesta coordinada a nivel internacional.

- Campañas de concientización: Se han llevado a cabo campañas de concientización y educación en materia de ciberseguridad en México, tanto a nivel gubernamental como en el sector privado y la sociedad civil. Estas campañas buscan sensibilizar a la población sobre los riesgos del ciberdelito, promover buenas prácticas de seguridad en línea y fomentar una cultura de ciberseguridad en la sociedad mexicana. La concientización es un componente importante en la prevención del ciberdelito, ya que permite a los usuarios adoptar medidas de seguridad adecuadas y evitar caer víctimas de estos delitos.

Desafíos en la regulación del ciberdelito en México:

- Evolución tecnológica: La rápida evolución de la tecnología representa un desafío constante en la regulación del ciberdelito. Los delincuentes cibernéticos utilizan técnicas sofisticadas y cambiantes, lo que dificulta la detección y persecución de los delitos cibernéticos. La regulación del ciberdelito debe adaptarse constantemente a los avances tecnológicos para poder enfrentar eficazmente las nuevas modalidades de delitos que surgen en el entorno digital, como el robo de información, el phishing, el ransomware, entre otros.

- Falta de recursos técnicos y tecnológicos: Aunque se ha avanzado en la creación de instituciones especializadas en la atención del ciberdelito, aún existe una falta de recursos técnicos y tecnológicos necesarios para enfrentar los retos del ciberespacio. La capacitación de personal especializado en el uso de tecnologías forenses, análisis de datos y ciberseguridad, así como la adquisición de herramientas tecnológicas avanzadas, son necesidades urgentes para mejorar la eficacia en la persecución del ciberdelito.

- Retos en la cooperación internacional: Aunque se ha fortalecido la cooperación internacional en la lucha contra el ciberdelito, aún existen desafíos en este ámbito. La extradición de delincuentes cibernéticos, el intercambio de información y la colaboración en investigaciones transnacionales pueden enfrentar obstáculos legales y tecnológicos, lo que dificulta la persecución efectiva de los delitos cibernéticos que cruzan fronteras.

- Subregistro y falta de denuncias: Uno de los desafíos en la regulación del ciberdelito es el subregistro y la falta de denuncias por parte de las víctimas. Muchas veces, las víctimas de delitos cibernéticos no denuncian por temor a represalias, falta de confianza en las autoridades o desconocimiento de los procedimientos para reportar estos delitos. Esto dificulta la identificación y persecución de los delincuentes cibernéticos, así como la obtención de datos estadísticos precisos sobre la magnitud del problema.

- Complejidad en la atribución y jurisdicción: La naturaleza global del ciberdelito y la posibilidad de cometer delitos desde diferentes ubicaciones geográficas dificulta la atribución y jurisdicción de los delitos cibernéticos. La identificación de los autores de los delitos, la determinación de la jurisdicción aplicable y la coordinación entre distintas instancias y países pueden ser complicadas y retrasar el proceso de persecución y sanción de los delincuentes cibernéticos.

- Actualización legislativa: Aunque México cuenta con un marco jurídico específico para la regulación del ciberdelito, es necesario realizar constantes actualizaciones legislativas para adaptarse a la evolución del entorno digital y las nuevas modalidades de delitos cibernéticos. Es importante asegurar que las leyes sean claras, efectivas y proporcionales, y que brinden herramientas adecuadas a las autoridades para la prevención, persecución y sanción del ciberdelito.

- Coordinación interinstitucional: La coordinación entre distintas instituciones gubernamentales y organismos involucrados en la regulación del ciberdelito puede ser un desafío. La colaboración entre la Fiscalía General de la República, la Secretaría de Seguridad y Protección Ciudadana, la Secretaría de Comunicaciones y Transportes, entre otras instituciones, así como la participación activa del sector privado y la sociedad civil, es esencial para enfrentar eficazmente el ciberdelito, sin embargo, la falta de una coordinación adecuada puede generar duplicidad de esfuerzos, falta de claridad en los roles y responsabilidades, y debilidades en la implementación de estrategias integrales de prevención y combate del ciberdelito.

- Desafíos en la educación y concientización: La educación y concientización en temas de ciberseguridad son fundamentales para prevenir el ciberdelito, sin embargo, aún existe una falta de conciencia y conocimiento en la población sobre los riesgos y medidas de protección en el entorno digital, es necesario fortalecer la educación en ciberseguridad desde edades tempranas, así como desarrollar campañas de

concientización dirigidas a diferentes sectores de la sociedad, incluyendo a empresas, organizaciones gubernamentales y ciudadanía en general.

- Retos en la protección de datos personales: La protección de datos personales es un aspecto crucial en la regulación del ciberdelito, ya que muchos delitos cibernéticos involucran la obtención, uso o divulgación no autorizada de datos personales, aunque México cuenta con una ley específica de protección de datos personales, aún existen desafíos en su implementación y cumplimiento, es necesario fortalecer la protección de datos personales, promover buenas prácticas en su manejo y concientizar a la población sobre la importancia de proteger su información en línea.

- Retos en la prevención y atención a víctimas: La prevención y atención a las víctimas de ciberdelito son aspectos importantes en la regulación del ciberdelito, sin embargo, aún existen desafíos en este ámbito, incluyendo la falta de programas integrales de prevención, la atención adecuada a las víctimas y la reparación del daño. Es necesario implementar estrategias de prevención del ciberdelito que incluyan medidas técnicas, educativas y sociales, así como garantizar una atención adecuada y oportuna a las víctimas, incluyendo su protección, asesoría y apoyo en el proceso de denuncia y persecución de los delitos cibernéticos.

Por lo tanto, si bien México ha avanzado en la regulación y prevención del ciberdelito, aún enfrenta diversos desafíos y superarlos requerirá de un enfoque integral que involucre la participación activa de las autoridades, el sector privado, la sociedad civil y la ciudadanía en general, así como una constante adaptación a los avances tecnológicos y a las nuevas modalidades de delitos cibernéticos.

4.2 Legislación sobre los ciberdelitos en México

La tipificación de los ciberdelitos en México se encuentra regulada principalmente en el Código Penal Federal y en los Códigos Penales Estatales del país, estas normativas

establecen los delitos cibernéticos y las sanciones correspondientes para aquellos que los cometan; a continuación, se presenta un análisis detallado de la tipificación de los ciberdelitos en la legislación mexicana.

Código Penal Federal, en el capítulo II "Acceso ilícito a sistemas y equipos de informática", publicado en el Diario Oficial de la Federación de fecha: 17-05-1999, contempla diversos tipos de ciberdelitos, entre los que se encuentran:

- Acceso ilícito a sistemas y equipos informáticos: Se sanciona a aquel que acceda, copie, destruya, altere, modifique o utilice indebidamente sistemas, programas informáticos o equipos de procesamiento electrónico de datos sin contar con la autorización correspondiente.

- Daño en sistemas y equipos informáticos: Se castiga al que dañe, destruya, inutilice o altere sistemas, programas informáticos o datos contenidos en equipos de procesamiento electrónico de datos, sin contar con la autorización correspondiente.

- Sabotaje informático: Se sanciona al que destruya, inutilice, dañe, altere o interrumpa total o parcialmente sistemas, programas informáticos o datos contenidos en equipos de procesamiento electrónico de datos con el fin de causar un perjuicio.

- Fraude informático: Se castiga a quien, con fines de lucro, obtenga un beneficio indebido para sí o para otro, induciendo o manteniendo a una persona en error mediante el uso de tecnologías de la información.

- Daño a datos o programas informáticos ajenos: Se sanciona a aquel que destruya, dañe, inutilice, altere o borre datos o programas informáticos ajenos.

- Falsificación de documentos electrónicos: Se castiga a quien, con ánimo de perjudicar o causar un perjuicio a otro, falsifique, modifique o altere documentos electrónicos.

- Pornografía infantil: Se sanciona a quien produzca, reproduzca, distribuya, posea, adquiera, importe, exporte, venda, arriende, exhiba, transmita, comparta, publicite o publique imágenes, material o representaciones pornográficas de personas menores de 18 años.

- Amenazas y extorsión informática: Se castiga a quien amenace o extorsione a otro utilizando tecnologías de la información, ya sea exigiendo la revelación de información confidencial, el pago de una suma de dinero o la realización de un acto en perjuicio de la víctima.

- Delitos contra la propiedad intelectual e industrial: Se sanciona a quien realice actos de reproducción, distribución, venta o almacenamiento de obras protegidas por derechos de autor o de marcas registradas sin contar con la debida autorización.

- Delitos electorales en línea: Se castiga a quien realice acciones ilegales en el ámbito electoral a través de tecnologías de la información, como la difusión de noticias falsas, la suplantación de identidad, la compra de votos o la alteración de resultados electorales.

Es importante destacar que los delitos cibernéticos están clasificados como delitos federales en México, lo que significa que son competencia de la Fiscalía General de la República (FGR) y se rigen por el Código Penal Federal, sin embargo, algunos estados también cuentan con legislación específica en sus Códigos Penales Estatales para tipificar y sancionar los ciberdelitos.

Además, en México, la legislación vigente contempla los ciberdelitos contra la confidencialidad, integridad y disponibilidad de datos como conductas ilícitas que pueden ser sancionadas, estos delitos afectan la seguridad y privacidad de la información almacenada o transmitida a través de medios electrónicos, y son considerados como una amenaza a la integridad del ciberespacio y a la confianza en el uso de las tecnologías de la información.

La regulación de los ciberdelitos contra la confidencialidad, integridad y disponibilidad de datos en México se encuentra establecida principalmente en el Código Penal Federal y en algunos Códigos Penales Estatales; estos delitos se tipifican como conductas ilícitas que atentan contra la seguridad y funcionamiento de sistemas informáticos, la confidencialidad de la información almacenada en dichos sistemas, así como la integridad y disponibilidad de los datos.

En el Código Penal Federal (2020), se establecen diversas conductas que constituyen ciberdelitos contra la confidencialidad, integridad y disponibilidad de datos, entre las cuales se encuentran:

- Acceso ilícito a sistemas y equipos de informática: Se considera delito el acceso sin autorización a sistemas o equipos de informática, o permanecer en ellos una vez obtenido el acceso sin autorización. Esta conducta es sancionada con pena de prisión y multa.

- Interceptación ilícita de datos: Se considera delito la interceptación o interrupción de la transmisión de datos electrónicos sin autorización. Esta conducta es sancionada con pena de prisión y multa.

- Daño a sistemas y equipos de informática: Se considera delito causar daño o alteración a sistemas o equipos de informática, así como a programas o datos almacenados en ellos. Esta conducta es sancionada con pena de prisión y multa.

- Sabotaje informático: Se considera delito el sabotaje informático, que consiste en el uso de programas o datos informáticos para causar daño, alteración o destrucción de sistemas, equipos o datos informáticos. Esta conducta es sancionada con pena de prisión y multa.

- Espionaje informático: Se considera delito el acceso ilícito a sistemas o equipos de informática con el fin de obtener información confidencial o secreta. Esta conducta es sancionada con pena de prisión y multa.

Las sanciones previstas en la legislación mexicana para los ciberdelitos contra la confidencialidad, integridad y disponibilidad de datos varían dependiendo de la gravedad de la conducta, pudiendo ir desde penas de prisión de uno a diez años, y multas que pueden alcanzar montos considerables, además, se prevé la confiscación de los instrumentos, programas o datos utilizados en la comisión del delito.

Es importante destacar que la legislación mexicana también contempla la agravación de las penas cuando los ciberdelitos son cometidos con fines de lucro, en perjuicio de entidades públicas, en perjuicio de la seguridad nacional, o cuando involucran a menores de edad, entre otras circunstancias agravantes.

Por otra parte, la ciberextorsión, chantaje y amenazas son formas de ciberdelitos que afectan la seguridad y privacidad de las personas y organizaciones en México, estos delitos involucran el uso de medios electrónicos para obtener beneficios económicos o causar daño a través de la coacción o intimidación, la regulación de estos delitos en México se encuentra establecida en el Código Penal Federal y en algunos Códigos Penales Estatales, y su análisis es fundamental en el marco de la legislación sobre ciberdelitos en el país, algunas de las conductas que se consideran como ciberextorsión, chantaje y amenazas en la legislación vigente son las siguientes:

- Extorsión electrónica: Se considera delito la obtención de bienes, dinero o cualquier otro beneficio económico mediante el uso de medios electrónicos, ya sea a través de la intimidación, amenaza, coacción o violencia. Esta conducta es sancionada con pena de prisión y multa, y las penas se agravan cuando se utilizan datos personales o se comete en perjuicio de una entidad pública o de una persona en situación de vulnerabilidad.

- Chantaje cibernético: Se considera delito el uso de medios electrónicos para amenazar con revelar información o difundir datos sensibles o comprometedores, con el fin de obtener un beneficio económico o causar daño a otra persona. Esta conducta es sancionada con pena de prisión y multa, y las penas se agravan cuando se comete en perjuicio de una persona en situación de vulnerabilidad.

- Amenazas por medios electrónicos: Se considera delito el uso de medios electrónicos para amenazar con causar un daño a una persona, a su familia o a su patrimonio. Esta conducta es sancionada con pena de prisión y multa, y las penas se agravan cuando se utilizan datos personales o se comete en perjuicio de una persona en situación de vulnerabilidad.

La legislación mexicana también prevé la agravación de las penas cuando los delitos de ciberextorsión, chantaje y amenazas son cometidos en perjuicio de entidades públicas, cuando involucran a menores de edad, o cuando se cometen en el marco de una organización criminal, entre otras circunstancias agravantes.

Es importante destacar que la legislación mexicana también establece la responsabilidad de las personas jurídicas, incluyendo a las empresas y organizaciones, en caso de comisión de ciberdelitos como la ciberextorsión, chantaje y amenazas, las empresas pueden ser sancionadas con multas y otras medidas, incluyendo la clausura o suspensión de sus actividades, cuando se comprueba su participación o negligencia en la comisión de estos delitos, además de las sanciones

penales, la legislación mexicana también prevé medidas de prevención y protección en casos de ciberextorsión, chantaje y amenazas. Esto incluye la posibilidad de solicitar medidas de protección a la autoridad, como la restricción de acceso a determinados medios electrónicos o la protección de datos personales, así como la obligación de las autoridades de brindar apoyo y protección a las personas afectadas por estos delitos.

Por lo tanto, es esencial contar con una legislación actualizada y adecuada, así como con capacidades técnicas y operativas en las autoridades encargadas de la aplicación de la ley, para hacer frente a estos desafíos y garantizar la efectiva prevención, persecución y sanción de los ciberdelitos en México.

4.3 Control y prevención de delitos cibernéticos

El combate al ciberdelito en México no se limita únicamente a la legislación y sanciones, sino que también implica la implementación de políticas y estrategias de prevención que buscan minimizar los riesgos y promover una cultura de seguridad cibernética en la sociedad; en los últimos años, México ha implementado diversas políticas y estrategias de prevención del ciberdelito, tanto a nivel federal como estatal, como señala la American Chamber of Commerce of Mexico en un artículo, *"la Estrategia Nacional de Ciberseguridad debe ser una política pública vinculada a la protección de la seguridad nacional ya que inclusive la seguridad del Estado está en juego"*. Estas políticas buscan crear conciencia sobre la importancia de la seguridad cibernética, promover mejores prácticas en el uso de las tecnologías de la información, y fortalecer la protección de los datos personales y la información en línea, algunas de las principales políticas y estrategias implementadas en México son:

- Estrategia Nacional de Ciberseguridad: Esta estrategia, implementada por el Gobierno Federal, busca fortalecer la ciberseguridad en México a través de la coordinación de esfuerzos entre diferentes dependencias gubernamentales, la promoción de la colaboración público-privada, y la creación de políticas y regulaciones

en materia de ciberseguridad. La estrategia incluye acciones para la prevención, detección, respuesta y recuperación de incidentes cibernéticos, así como la capacitación y concientización de la población.

- Programas de capacitación y concientización: Se han implementado programas de capacitación y concientización en materia de seguridad cibernética, tanto para el sector público como el sector privado y la sociedad en general. Estos programas buscan promover una cultura de seguridad cibernética, brindar conocimientos y herramientas para la prevención de ciberdelitos, y fomentar mejores prácticas en el uso de la tecnología.

- Fortalecimiento de capacidades técnicas y operativas: Se han realizado esfuerzos para fortalecer las capacidades técnicas y operativas de las autoridades encargadas de la aplicación de la ley en materia de ciberseguridad. Esto incluye la formación de unidades especializadas en delitos cibernéticos, la adopción de tecnologías y herramientas para la detección y respuesta a incidentes cibernéticos, y la promoción de la colaboración internacional en la lucha contra el ciberdelito.

- Protección de datos personales: La protección de datos personales es un componente importante de las políticas de prevención del ciberdelito en México. Se han implementado regulaciones y normativas en materia de privacidad y protección de datos, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010), que establece los principios y obligaciones para el tratamiento de datos personales, así como los derechos de los titulares de datos.

- Cooperación internacional: México ha buscado fortalecer la cooperación internacional en la lucha contra el ciberdelito, a través de la participación en organismos internacionales, acuerdos bilaterales y multilaterales, y la promoción de la colaboración con otros países en la prevención, investigación y sanción de los

ciberdelitos. La cooperación internacional es fundamental en la lucha contra el ciberdelito, dada la naturaleza transnacional de estos delitos.

Es importante destacar que México ha avanzado en la implementación de políticas y estrategias de prevención del ciberdelito, buscando fortalecer la seguridad cibernética y proteger a los usuarios de tecnología en el país, sin embargo, aún queda trabajo por hacer en la concientización y educación de la sociedad sobre la importancia de la seguridad cibernética, así como en el fortalecimiento de capacidades técnicas y operativas de las autoridades encargadas de la aplicación de la ley.

El entorno digital está en constante evolución y presenta diversos desafíos en términos de seguridad y protección. En México, se han implementado varias medidas de seguridad y protección en el entorno digital con el objetivo de prevenir y combatir los delitos cibernéticos. A continuación, se describen algunas experiencias y buenas prácticas en México en este contexto:

- Campañas de concientización y educación: La concientización y educación son elementos clave en la prevención de delitos cibernéticos. En México, se han llevado a cabo diversas campañas de concientización y educación dirigidas a la población en general, así como a sectores específicos como niños, adolescentes, padres de familia, empresas y servidores públicos, estas campañas buscan promover buenas prácticas de seguridad cibernética, como el uso de contraseñas seguras, la protección de la información personal, la identificación y prevención de phishing, y la promoción de la cultura de seguridad en línea.

- Fortalecimiento de capacidades técnicas y operativas: Las autoridades encargadas de la aplicación de la ley en México han buscado fortalecer sus capacidades técnicas y operativas en materia de ciberseguridad. Esto incluye la capacitación y formación del personal en técnicas forenses digitales, análisis de malware, respuesta a incidentes, y otros aspectos relacionados con la seguridad cibernética, además, se han

implementado herramientas y tecnologías avanzadas para la detección y prevención de ciberataques, así como la cooperación con otros países y organismos internacionales para el intercambio de información y mejores prácticas en la lucha contra los delitos cibernéticos.

- Legislación y regulación actualizada: México cuenta con una legislación y regulación actualizada en materia de ciberseguridad y delitos cibernéticos. Leyes como la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y el Código Penal Federal, entre otros, establecen las normas y sanciones aplicables a los delitos cibernéticos, así como las obligaciones y responsabilidades de los actores involucrados en el entorno digital, estas leyes buscan proporcionar un marco legal sólido para prevenir, sancionar y combatir los delitos cibernéticos en México.

- Colaboración entre sectores público y privado: La colaboración entre el sector público y privado es esencial en la prevención de delitos cibernéticos. En México, se han establecido mecanismos de colaboración y coordinación entre el gobierno, las empresas, las organizaciones de la sociedad civil y otros actores involucrados en el entorno digital, esto incluye la creación de comités, grupos de trabajo y plataformas de intercambio de información, así como la promoción de la participación activa de la sociedad civil y el sector privado en la identificación y prevención de delitos cibernéticos.

- Desarrollo de capacidades locales: México ha buscado fortalecer las capacidades locales en materia de ciberseguridad a través de la promoción de la investigación, desarrollo y capacitación en el país. Esto incluye la creación de programas de formación en ciberseguridad, la promoción de la investigación y desarrollo de tecnologías de seguridad cibernética, y la participación activa de instituciones educativas y de investigación en la generación de conocimiento y buenas prácticas en este campo, en consecuencia, se han impulsado iniciativas para fomentar la creación de empresas y startups especializadas en ciberseguridad, con el objetivo de promover

la innovación y el desarrollo de soluciones tecnológicas para la protección del entorno digital.

En general, México ha implementado diversas medidas de seguridad y protección en el entorno digital, incluyendo campañas de concientización, fortalecimiento de capacidades técnicas y operativas, legislación y regulación actualizada, colaboración entre sectores públicos y privado, desarrollo de capacidades locales, protección de infraestructuras críticas, y participación en organismos internacionales. Sin embargo, es importante destacar que la efectividad de estas medidas en la prevención del ciberdelito puede variar y enfrentar desafíos en términos de implementación, coordinación, recursos y actualización constante frente a la evolución de las amenazas cibernéticas, por lo tanto, es fundamental que las políticas y estrategias de prevención del ciberdelito en México sean evaluadas y actualizadas de forma continua para garantizar su eficacia en la protección del entorno digital y la seguridad de los usuarios en línea.

La educación y concientización en ciberseguridad han sido componentes fundamentales de las estrategias implementadas en México para el control y prevención de delitos cibernéticos, se han llevado a cabo diversos programas y estrategias para promover la conciencia sobre la importancia de la seguridad en línea, capacitar a los usuarios en prácticas seguras y fomentar el uso responsable de la tecnología en el entorno digital.

Uno de los principales enfoques de la educación y concientización en ciberseguridad en México ha sido dirigido a la población en general, con un enfoque especial en los niños, adolescentes y jóvenes, que son considerados un grupo vulnerable ante las amenazas cibernéticas; se han implementado programas en escuelas, comunidades y medios de comunicación para promover la importancia de proteger la información personal, evitar la divulgación de datos sensibles en línea, y prevenir el acceso a contenido inapropiado o peligroso, estos programas incluyen charlas, talleres,

materiales educativos, y campañas de concientización en medios de comunicación masiva para promover la cultura de la ciberseguridad.

Además, se han implementado estrategias de capacitación en ciberseguridad dirigidas a diversos sectores de la sociedad, como funcionarios públicos, empresas, organizaciones de la sociedad civil, y usuarios en general, estas capacitaciones incluyen temas como la protección de datos personales, la identificación de amenazas cibernéticas, la prevención de la ciberextorsión, y la adopción de prácticas seguras en el uso de dispositivos y servicios en línea; dichos programas de capacitación se han llevado a cabo en forma de talleres, cursos, seminarios y conferencias, con la participación de expertos en ciberseguridad y la colaboración de instituciones gubernamentales, organizaciones de la sociedad civil y el sector privado.

Otro componente importante de la educación y concientización en ciberseguridad en México ha sido la promoción de buenas prácticas en el uso de tecnologías y servicios en línea. Se han desarrollado guías, manuales y recursos educativos para orientar a los usuarios sobre cómo proteger sus cuentas en redes sociales, evitar caer en fraudes en línea, proteger sus contraseñas, y mantener actualizados sus dispositivos y programas, estos recursos educativos se han distribuido ampliamente a través de plataformas en línea, medios de comunicación y campañas de concientización para promover la adopción de medidas de seguridad y protección en el entorno digital.

Asimismo, se han implementado campañas de concientización y prevención específicas en temas como el sexting, el grooming, el phishing, y la suplantación de identidad, con el objetivo de informar a los usuarios sobre los riesgos asociados a estas prácticas y promover la adopción de medidas de prevención, debido a todo lo descrito anteriormente, se destaca la importancia de una regulación adecuada y efectiva que se adapte a las cambiantes tecnologías y amenazas cibernéticas, así como a los estándares internacionales en la materia.

Se resalta la necesidad de fortalecer la cooperación internacional y la adopción de marcos normativos internacionales para enfrentar las amenazas cibernéticas de manera colaborativa, asimismo, se subraya la importancia de contar con una legislación actualizada y robusta en materia de ciberseguridad en México, que promueva la prevención, detección y sanción de los delitos cibernéticos de manera efectiva.

De la misma forma se puntualiza la necesidad de promover la educación y concientización en ciberseguridad, tanto en la sociedad como en las instituciones gubernamentales y el sector privado, como parte integral de la estrategia de prevención del ciberdelito; en cuanto al control y prevención de delitos cibernéticos, se enfatiza la importancia de implementar medidas integrales que involucren a diferentes actores, como el gobierno, el sector privado, la sociedad civil y la ciudadanía en general, esto incluye la implementación de políticas, programas y tecnologías que promuevan la seguridad cibernética, la detección temprana de amenazas, y la respuesta adecuada a los incidentes cibernéticos.

Derivado de las ideas antes mencionadas, se puede establecer la idea de que el Gobierno Federal de México en sus facultades establecidas en la legislación actual, promueva diversos programas de prevención de los distintos delitos cibernéticos, además de fomentar en la sociedad una cultura de denuncia.

Según un informe de Anice, si la ciberseguridad se logra regular y prevenir, se obtendrían los siguientes beneficios:

Figura 1: Beneficios de la ciberseguridad.

Fuente: Anice (2022).

PROPUESTAS

El ciberdelito es una amenaza creciente en el mundo digital, con consecuencias graves para la seguridad, la privacidad y la economía. México, al igual que muchos otros países, enfrenta desafíos en la regulación y prevención del ciberdelito, para hacer frente a esta problemática, se propone una serie de políticas y estrategias integrales que aborden los principales aspectos del ciberdelito y promuevan la seguridad en línea en México.

Los objetivos de la propuesta son:

PRIMERA: Fortalecer la legislación existente y desarrollar nuevas normativas que aborden de manera efectiva el ciberdelito en todas sus formas, incluyendo la ciberextorsión, el fraude electrónico, el robo de información, el acoso cibernético, la suplantación de identidad y otros delitos cibernéticos.

SEGUNDA: Mejorar la capacidad de respuesta y coordinación entre las autoridades encargadas de la prevención, investigación y sanción del ciberdelito, incluyendo a la policía cibernética, el Ministerio Público y el Poder Judicial, a través de la implementación de tecnologías avanzadas, la capacitación especializada y la colaboración con otros países y organismos internacionales.

TERCERA: Fomentar la colaboración y participación activa del sector privado, la sociedad civil, la academia y la comunidad en general, en la prevención y combate del ciberdelito, promoviendo la cultura de la ciberseguridad y concientizando a los usuarios sobre las mejores prácticas en línea.

CUARTA: Establecer mecanismos efectivos de prevención y protección en el entorno digital, incluyendo la implementación de medidas de seguridad y protección en infraestructuras críticas, la promoción de buenas prácticas en el uso de tecnologías y

servicios en línea, y la promoción de la adopción de políticas de seguridad en el sector público y privado.

Por lo tanto, las acciones de la propuesta son:

QUINTA: Fortalecimiento de la legislación: Se propone la revisión y actualización de la legislación existente para adecuarla a las nuevas formas de ciberdelito, así como el desarrollo de nuevas normativas que aborden aspectos específicos del ciberdelito, esto incluye la definición clara de los delitos cibernéticos, la asignación de sanciones adecuadas, la regulación de la obtención y uso de datos personales en línea, y la promoción de la cooperación internacional en el combate al ciberdelito.

SEXTA: Fortalecimiento de las capacidades de las autoridades: Se propone el fortalecimiento de las capacidades técnicas y operativas de las autoridades encargadas de la prevención, investigación y sanción del ciberdelito, esto incluye la implementación de tecnologías avanzadas para la detección y seguimiento de delitos cibernéticos, la capacitación especializada de los cuerpos de seguridad en técnicas de ciberinvestigación, y la creación de unidades especializadas en el combate al ciberdelito en la policía cibernética y el Ministerio Público.

SEPTIMA: Promoción de la colaboración y participación de actores clave: Se propone fomentar la colaboración y participación activa del sector privado, la sociedad civil, la academia y la comunidad en general en la prevención y combate del ciberdelito, objetivamente contiene la promoción de alianzas público-privadas para compartir información y buenas prácticas en ciberseguridad, la realización de campañas de concientización y educación en ciberseguridad dirigidas a diferentes sectores de la sociedad, la promoción de la participación de la academia en la investigación y desarrollo de soluciones tecnológicas para la prevención y combate del ciberdelito, y la creación de programas de capacitación y formación en ciberseguridad para el sector público y privado.

OCTAVA: Implementación de medidas de prevención y protección en el entorno digital: Se propone la implementación de medidas de prevención y protección en el entorno digital para fortalecer la seguridad en línea, contemplando la promoción de buenas prácticas en el uso de tecnologías y servicios en línea, como el uso de contraseñas seguras, la actualización regular de software y la protección de información sensible, así como la promoción de políticas de seguridad en el sector público y privado, incluyendo la implementación de sistemas de gestión de seguridad de la información, la protección de infraestructuras críticas, y la promoción de la seguridad en el desarrollo de aplicaciones y servicios en línea.

NOVENA: Cooperación internacional en el combate al ciberdelito: Se propone fortalecer la cooperación internacional en el combate al ciberdelito, a través de la promoción de acuerdos y convenios de colaboración con otros países y organismos internacionales, analizando la inclusión de la promoción de la extradición y persecución de delincuentes cibernéticos a nivel internacional, la colaboración en la identificación y seguimiento de actividades delictivas en línea, el intercambio de información y buenas prácticas en ciberseguridad, y la participación en foros y organizaciones internacionales dedicadas a la prevención y combate del ciberdelito.

La implementación de políticas y estrategias que fortalezcan la legislación, capaciten a las autoridades, promuevan la colaboración de actores clave, implementen medidas de prevención y protección en el entorno digital, y promuevan la cooperación internacional, puede contribuir a prevenir y combatir el ciberdelito en México.

Es fundamental promover una cultura de ciberseguridad, concientizar a los usuarios sobre las mejores prácticas en línea y fomentar la colaboración entre los diferentes actores involucrados para asegurar un entorno digital seguro y confiable para todos los ciudadanos mexicanos, con un enfoque integral y acciones concretas, México puede avanzar en la regulación y prevención del ciberdelito, protegiendo la seguridad, la privacidad y la economía en el entorno digital; con base en la propuesta presentada,

se hacen las siguientes recomendaciones para la regulación y prevención del ciberdelito en México:

DECIMA: Implementar programas de educación y concientización en ciberseguridad: La educación y concientización en ciberseguridad es esencial para prevenir el ciberdelito; se deben implementar programas de educación y concientización en ciberseguridad dirigidos a diferentes sectores de la sociedad, incluyendo a los ciudadanos, empresas, organizaciones gubernamentales y educativas. Estos programas deben abordar temas como el uso seguro de contraseñas, la protección de información sensible, la identificación de posibles amenazas en línea y el uso responsable de la tecnología, además, se deben promover campañas de concientización en medios de comunicación y redes sociales para sensibilizar a la población sobre los riesgos y consecuencias del ciberdelito.

DECIMA PRIMERA: Implementar medidas de prevención y protección en el entorno digital: Es fundamental implementar medidas de prevención y protección en el entorno digital para fortalecer la seguridad en línea, integrando buenas prácticas en el uso de tecnologías y servicios en línea, como el uso de contraseñas seguras, la actualización regular de software y la protección de información sensible; Además se deben promover políticas de seguridad en el sector público y privado, incluyendo la implementación de sistemas de gestión de seguridad de la información, la protección de infraestructuras críticas, y la promoción de la seguridad en el desarrollo de aplicaciones y servicios en línea, es importante también fomentar la adopción de tecnologías de seguridad, como firewalls, antivirus, cifrado de datos y soluciones de seguridad en la nube, en todos los niveles de la sociedad.

DECIMA SEGUNDA: Fomentar la investigación y desarrollo en ciberseguridad: La tecnología evoluciona rápidamente, y con ello también lo hacen las amenazas cibernéticas; es por ello fundamental fomentar la investigación y desarrollo en ciberseguridad en México, agregando la promoción de la formación y capacitación de expertos en ciberseguridad, la inversión en investigación y desarrollo de tecnologías y

herramientas de seguridad, y la promoción de la innovación en el campo de la ciberseguridad, además, se deben establecer mecanismos de apoyo a la industria de ciberseguridad en México, promoviendo la participación de empresas y startups en la creación de soluciones y servicios de ciberseguridad de vanguardia.

La implementación de estas medidas requiere de un enfoque holístico y multidisciplinario, que involucre a múltiples actores, incluyendo al gobierno, sector privado, sociedad civil, academia y ciudadanía en general, por lo que es necesario promover una cultura de ciberseguridad en todos los niveles, desde el ámbito educativo hasta el empresarial, y fomentar la responsabilidad compartida en la protección del entorno digital.

Además, es fundamental contar con recursos y capacidades técnicas adecuadas para enfrentar las amenazas cibernéticas, esto incluye la formación y capacitación de profesionales especializados en ciberseguridad, la inversión en tecnologías y herramientas de seguridad de vanguardia, y la promoción de la innovación en el campo de la ciberseguridad.

La cooperación internacional también juega un papel crucial en la lucha contra el ciberdelito, ya que muchas veces las amenazas cibernéticas trascienden las fronteras y requieren de acciones coordinadas a nivel global. México debe establecer alianzas y acuerdos de colaboración con otros países, organizaciones internacionales y agencias especializadas en ciberseguridad, con el fin de compartir información, mejores prácticas y recursos en la prevención, detección, investigación y persecución del ciberdelito.

Por lo tanto, la propuesta para la regulación y prevención del ciberdelito en México presenta un enfoque integral y proactivo para abordar los desafíos actuales y futuros en el ámbito de la ciberseguridad; a través de la implementación de políticas y estrategias basadas en la colaboración, la educación y la tecnología, se busca

fortalecer la legislación existente, promover la prevención y protección en el entorno digital, fomentar una cultura de ciberseguridad, y fomentar la cooperación internacional.

La propuesta destaca la necesidad de una legislación actualizada y robusta que aborde los delitos cibernéticos de manera efectiva, adaptándose a las cambiantes tecnologías y amenazas en el ciberespacio, es por este motivo que se enfatiza la importancia de la colaboración entre el gobierno, el sector privado, la sociedad civil, la academia y la ciudadanía en general, para trabajar de manera conjunta en la prevención, detección y respuesta al ciberdelito; la educación y concientización en ciberseguridad son elementos fundamentales de la propuesta, reconociendo que una sociedad bien informada y consciente de los riesgos cibernéticos está mejor preparada para protegerse a sí misma y a sus activos digitales, se proponen programas y estrategias de educación y concientización en todos los niveles, desde la educación temprana hasta el ámbito empresarial, con el objetivo de promover una cultura de ciberseguridad que fomente la responsabilidad compartida y la adopción de buenas prácticas en el uso de la tecnología.

La propuesta también destaca la importancia de la cooperación internacional en la lucha contra el ciberdelito, reconociendo la naturaleza transnacional de muchas amenazas cibernéticas; se plantea la necesidad de establecer alianzas y acuerdos de colaboración con otros países y organizaciones internacionales, con el fin de compartir información, buenas prácticas y experiencias en la prevención y combate al ciberdelito; por lo tanto, la propuesta para la regulación y prevención del ciberdelito en México busca abordar de manera integral los retos y desafíos en el ámbito de la ciberseguridad, con un enfoque basado en la legislación, colaboración, educación y cooperación internacional. Con la implementación de estas medidas, se busca promover un entorno digital seguro y confiable en México, protegiendo la seguridad y privacidad de los ciudadanos, empresas y el gobierno, y contribuyendo a la construcción de una sociedad digital resiliente y protegida frente a las amenazas cibernéticas.

CONCLUSIONES

PRIMERA: Creación de una Ley Federal para Prevenir y Sancionar los Delitos Informáticos en México, esto con la única finalidad de poder tener una legislación especializada en el tema.

SEGUNDA: Creación de una Fiscalía Especializada en Materia de Delitos Informáticos, por lo que sería necesario que la Fiscalía General de la Republica tuviera a bien crear dicha fiscalía especializada con la finalidad de tener todas las herramientas humanas para el investigación de dichos hechos delictivos.

TERCERA: La participación activa de México en los distintos foros internacionales que traten sobre los temas de delitos informáticos, ya que la tecnología es una herramienta global en la cual todos los países se ven afectados por este fenómeno social.

CUARTA: Creación de Tratados Internacionales en donde México sea parte fundamental para el apoyo y colaboración bilateral con los demás países, con la finalidad de perseguir de una manera más eficiente los sujetos que participan en los delitos informáticos y compartir información con los demás países miembros de los Tratados.

QUINTA: Actualizar de forma constante y especializada a los Ministerios Públicos de la Fiscalía General de la Republica con la finalidad de obtener el conocimiento necesario para poder perseguir los delitos informáticos.

SEXTA: La creación de una división especializada en la Agencia de Investigación Criminal de la Fiscalía General de la Republica con la finalidad de tener los conocimientos necesarios para la investigación de los delitos informáticos.

SEPTIMA: Implementación de una campaña social con la finalidad de dar a conocer la existencia de los delitos informáticos y de esta forma realizar planeaciones para la prevención de estos delitos.

OCTAVA: Que la Fiscalía General de la Republica implemente una plataforma digital para poder realizar las denuncias de los delitos informáticos de una forma pronta y expedita.

NOVENA: La creación de peritos expertos en toda el área de la informática que puedan ingresar a laborar en el área pericial de la Fiscalía General de la Republica, esto debido a que serán necesarios peritajes especializados en la materia para la integración de una carpeta de investigación.

DECIMA: La implementación de una asignatura que aborde los delitos informáticos en todos los planes de estudio de las distintas Universidades del país, para que los estudiantes tenga del conocimientos desde su formación académica de la existencia de estos delitos.

DECIMA PRIMERA: Fomentar la necesidad de una competente ciber seguridad en todos los sistemas de computación, de las diversas dependencias federales para combatir los delitos informáticos de los que pueden ser víctimas.

DECIMA SEGUNDA: Por último la difusión de por parte del Estado asi como de las sociedades civiles, de la existencia de estos delitos y la forma en las que se pueden prevenir desde la sociedad.

FUENTES DE CONSULTA

BIBLIOGRAFIA

- Grabosky, P., & Smith, R. G. (1998). Introduction: Global crime, global security, and the governance of cyberspace. In P. Grabosky & R. G. Smith (Eds.), Crime in the digital age: Controlling telecommunications and cyberspace illegalities (pp. 1-16). New Brunswick, NJ: Transaction Publishers.

- Berberena, E. (2018). El delito informático en el Código Penal Federal. Universidad Nacional Autónoma de México.

- Hernández-Muñoz, J. M., & Martínez-Ballesteros, M. (2019). El marco legal de la seguridad informática y la ciberseguridad en México. Revista de la Facultad de Derecho de México, 69(273), 129-155.

- Ponce, J. (2021). Análisis crítico del marco jurídico mexicano en materia de delitos informáticos. Revista de derecho, 38(1), 61-76.

- Berberena, L. (2018). El régimen penal de los delitos informáticos en México. En E. Gutiérrez, F. de la Mora, & A. Sierra (Coords.), Temas de Derecho Penal Económico (pp. 133-159). Instituto de Investigaciones Jurídicas, UNAM.

- Gómez, C. (2019). Delitos informáticos y su tipificación en el derecho penal mexicano. Revista Internacional de Derecho Penal, 7(13), 77-89.

- Ruiz, J. R. (2016). Los delitos informáticos en México. Un análisis del artículo 211 Bis 1 del Código Penal Federal. Revista de Derecho Informático, (19), 65-88.

- Hernández-Muñoz, A., & Martínez-Ballesteros, M. (2019). Ciberseguridad y delitos informáticos: análisis de la normativa aplicable en México. Revista Internacional de Derecho y Ciencias Sociales, 2(2), 201-218.

- Vives Antón, T. (2002). Delitos informáticos: concepto y tipificación. Actualidad Penal, (10), 91-105.

- Montiel, J. (2018). Delitos informáticos: estudio doctrinal y jurisprudencial. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.

- Massón, M. D. (2015). Los delitos informáticos. Cizur Menor: Thomson Reuters Aranzadi.

- Hernández, R. (2014). Delitos informáticos y seguridad de la información. Pearson Educación.

- Tapia-Fonllem, C. (2014). Delitos informáticos cometidos por empleados. Investigación y Ciencia, (23), 38-45.

- Peguera, M. (2018). Cibercrimen y derecho: Los delitos informáticos en la sociedad de la información. Aranzadi.

- López-Tarruella Martínez-Conde, E. (2002). Delitos informáticos. Marcial Pons.

- López-Tarruella Martínez-Conde, E. (2002). El tratamiento penal de los delitos informáticos. Bosch.

- López-Tarruella Martínez-Conde, P. (2002). Delitos informáticos y propiedad intelectual. Dykinson.

- Hernández-Muñoz, A., & Martínez-Ballesteros, C. (2019). Delitos informáticos en México: análisis crítico del marco legal. Revista de Derecho Privado, (36), 33-60.

- Berberena, C. E. (2018). Delitos informáticos: Un reto para la protección de los derechos humanos. Revista Jurídica De La Universidad De Palermo, (26), 47-61.

- Gómez, A., & Álvarez, D. (2017). Delitos informáticos: Análisis de sujetos y problemáticas. Revista de Investigación Académica, 20, 1-14.

CIBERGRAFÍA

- American Chamber of Commerce of Mexico. (2019). Estrategia de Ciberseguridad en México. Recuperado el 16 de abril de 2023, de https://www.amcham.org.mx/sites/default/files/publications/VF_Estrategia%20de%20Ciberseguridad%20en%20Me%CC%81xico%20(1).pdf

- Amnesty International. (s. f.). Tratados internacionales. Recuperado el 15 de octubre de 2021, de https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/tratados-internacionales/

- Anice. (2022). La ciberseguridad centra el último seminario de Anice. Interempresas.net. https://www.interempresas.net/Industria-Carnica/Articulos/313803-La-ciberseguridad-centra-el-ultimo-seminario-de-Anice.html

- Biblioteca del Congreso Nacional de Chile. (2018). Convenio de Budapest y Ciberdelincuencia en Chile [PDF]. Biblioteca del Congreso Nacional de Chile.

https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf

- Cámara de Diputados del H. Congreso de la Unión. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares [PDF]. Recuperado el 16 de abril de 2023, de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

- Cámara de Diputados del H. Congreso de la Unión. (2021). Ley Federal de Telecomunicaciones y Radiodifusión. Recuperado el 16 de abril de 2023, de http://www.diputados.gob.mx/LeyesBiblio/ref/lftr.htm

- Código Penal Federal. (1 de julio de 2020). Diario Oficial de la Federación. Recuperado el 16 de abril de 2023, de https://dof.gob.mx/nota_detalle.php?codigo=5596005&fecha=01/07/2020

- Consejo de Europa. (2001). Convenio de Budapest sobre la ciberdelincuencia. Recuperado el 16 de abril de 2023, de https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

- Organización de los Estados Americanos. (1996). Convención Interamericana contra la Corrupción. Recuperado el 16 de abril de 2023, de https://www.gob.mx/cms/uploads/attachment/file/398264/convencion_interamericana_contra_la_corrupcion.pdf

- Pérez, S. A. R., & Pérez, S. A. R. (2021, 27 julio). Ciberdelitos: tratados internacionales y normativa nacional - Revista Consultoría. Revista Consultoría. https://revistaconsultoria.com.mx/ciberdelitos-tratados-internacionales-normativa-nacional/

- Secretaría De Relaciones Exteriores. (s. f.). Estrategia de Seguridad de Centroamérica (ESCA). gob.mx. https://www.gob.mx/sre/acciones-y-programas/estrategia-de-seguridad-de-centroamerica-esca?idiom=es

- United Nations Office on Drugs and Crime. (s. f.). Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y Sus Protocolos. https://www.unodc.org/toc/es/facts/convention/index.html

- Acosta, M. G. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. https://www.redalyc.org/journal/290/29062641023/html/

- Acurio Del Pino, S. (s.f.). Delitos Informáticos: Generalidades. Recuperado el 14 de abril de 2023, de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

- Badillo, D. (2022, 20 junio). México ocupa el octavo lugar en suplantación de identidad: IQSEC. El Economista. https://www.eleconomista.com.mx/sectorfinanciero/Mexico-ocupa-el-octavo-lugar-en-suplantacion-de-identidad-IQSEC-20220620-0044.html

- Cueto, H. (2022, 21 abril). Fraude en comercio electrónico subió 220% en México en la pandemia. Business Insider México | Noticias pensadas para ti. https://businessinsider.mx/fraude-comercio-electronico-mexico-sube-en-pandemia_tecnologia/

- Delitos Informáticos. (s.f.). Tipos de delitos informáticos. https://www.delitosinformaticos.info/delitos_informaticos/tipos_de_delitos/

- Escuela Judicial del Consejo de la Judicatura Federal. (2019). Delitos informáticos. Recuperado el 14 de abril de 2023, de https://escuelajudicial.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

- García, J. A. (2019). Delitos informáticos: impunidad organizacional y su impacto en la economía digital. Revista de la Facultad de Derecho y Ciencias Sociales, (47), 23-38. Recuperado de https://www.redalyc.org/journal/290/29062641023/html/

- Gobierno de México. (s.f.). Unidad Especializada en Delitos Fiscales y Financieros (UEIDFF). Recuperado el 14 de abril de 2023, de https://www.gob.mx/fgr/acciones-y-programas/la-unidad-especializada-en-delitos-fiscales-y-financieros-ueidff

- Infobae. (2023, 13 enero). Cayó sujeto por presuntamente haber producido casi 500 materiales de pornografía infantil en Nayarit. infobae. https://www.infobae.com/america/mexico/2023/01/13/cayo-sujeto-por-presuntamente-haber-producido-casi-500-materiales-de-pornografia-infantil-en-nayarit/

- Instituto IL&CJ. (2023, 14 de abril). [Mensaje en una página de Facebook]. Facebook. Recuperado el 14 de abril de 2023, de https://www.facebook.com/instituto.ilcj/photos/a.2080900385479780/3330852823817857/?locale=ms_MY

- Jurides. (2023). El error de tipo y el error de prohibición en Derecho Penal. Jurides • Asesoramiento Legal y Abogados Online. https://www.jurides.com/error-de-tipo-y-error-de-prohibicion-en-derecho-penal/

- Legislación SCJN. (s.f.). Buscador de Legislación SCJN. Recuperado el 14 de abril de 2023, de https://legislacion.scjn.gob.mx/Buscador/Paginas/wfArticuladoResultadoBusqueda.aspx?q=Zjujyqyrt96VrJeY7TvcvpKnFvecW01aT/1v9+3Wiw+8vp3l1liKmAuH1yBFWBTrAo155qtzwXCJtcyFbUJlMHZyLNczuJo0Bc/6EyvrPsnzbdaPSxNkvoR5SngW8iOg9zVNu14aGluiOOybjY/t5w==

- Ley especial contra los Delitos Informáticos. (2001). Ley especial contra los Delitos Informáticos (2001). Observatorio annaObserva http://www.annaobserva.org/observatorio/ley-especial-contra-delitos-informaticos-2001/

- Mayer Lux, Laura. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Ius et Praxis, 24(1), 159-206. https://dx.doi.org/10.4067/S0718-00122018000100159

- Mya Jurídico. (2022, mayo 30). Los elementos de la culpabilidad [Publicación de blog]. Recuperado el 14 de abril de 2023, de https://myajuridico.wordpress.com/2022/05/30/los-elementos-de-la-culpabilidad/

- Naturaleza Jurídica de los delitos informáticos. (s.f.). UNAM. Recuperado 14 de abril de 2023, de http://ru.juridicas.unam.mx/xmlui/handle/123456789/31543

- Orca, E. (s. f.). 3 casos reales de delitos informáticos en México. https://blog.orcagrc.com/casos-de-delitos-informaticos-en-mexico

- Parra, J. H. R. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. https://www.redalyc.org/journal/5177/517752176020/html/

- Riquelme, R. (2022, 26 julio). Ataques de ransomware afectan cadenas de suministro en México. El Economista. https://www.eleconomista.com.mx/tecnologia/Ataques-de-ransomware-afectan-cadenas-de-suministro-en-Mexico-20220726-0060.html

- Sicol Policía Nacional. (2022). Iter Criminis o camino del delito. Sicol Policía Nacional. https://sicol.es/iter-criminis-o-camino-del-delito/

- UNAM. (s. f.). Revista .Seguridad. UNAM. https://revista.seguridad.unam.mx/numero26/delitos-inform-ticos-en-m-xico

- Chouza-Calo, J. D., & Gómez-García, J. (2019). Perception of cybersecurity risks in Mexico: A study of organizational and personal behaviors. International Journal of Information Management, 49, 146-157. https://doi.org/10.1016/j.ijinfomgt.2019.06.006

- Organización de las Naciones Unidas. (2013). Informe de la Secretaría sobre delitos informáticos y prevención del delito. https://undocs.org/es/A/68/167

- Oficina de las Naciones Unidas contra la Droga y el Delito. (2018). Informe mundial sobre la delincuencia organizada transnacional. Delitos informáticos. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2018_esp.pdf

- Comisión Europea. (2018). Delitos informáticos y ciberseguridad. https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20180413_factsheet_cybersecurity_es.pdf

- Hwang, J., Cho, K., Kim, K., & Lee, J. (2018). Cybercrime definition and classification: A multidimensional model. Computers & Security, 76, 64-77. https://doi.org/10.1016/j.cose.2018.02.001

- Secretaría de Gobernación. (2020). Ley Federal de Delitos Informáticos. https://www.diputados.gob.mx/LeyesBiblio/pdf/6_070321.pdf

- Ponce, A. (2021). Análisis crítico del marco legal mexicano sobre ciberseguridad y delitos informáticos. Revista Digital de Derecho Administrativo, (29), 1-17. https://doi.org/10.18601/21452946.n29.01

- Ponce, A. (2021). Delitos informáticos en México: ¿qué tan eficaz es el marco legal? El Universal. Recuperado de https://www.eluniversal.com.mx/opinion/alexia-ponce/delitos-informaticos-en-mexico-que-tan-eficaz-es-el-marco-legal

- Código Penal Federal de México. (2021). Artículo 15. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/9_270621.pdf

- Código Penal Federal (México). (2021). Última reforma DOF 14-07-2021. https://www.diputados.gob.mx/LeyesBiblio/pdf/9_140721.pdf

- Symantec. (2019). Understanding Hackers and How They Operate. Recuperado de https://www.symantec.com/content/dam/symantec/docs/reports/understanding-hackers-and-how-they-operate-2019-en.pdf

- Acosta, F. y García, F. (2018). Delitos informáticos en México. Revista de Derecho y Ciencias Sociales, 1(1), 51-68.

- López-Tarruella Martínez-Conde, E. (2002). Delitos informáticos: concepto y regulación. Revista Electrónica de Estudios Jurídicos, (1), 1-23.

- Organización de los Estados Americanos. (2016). Estudio sobre el impacto de los delitos informáticos en las personas. Recuperado de https://www.oas.org/juridico/spanish/cyb_estudio_delitos_informaticos_personas.pdf