Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2024,
Volumen 8, Número 5.

https://doi.org/10.37811/cl_rcm.v8i5

DELITOS INFORMÁTICOS: UN TEMA DE ATENCIÓN LEGISLATIVA EN EL ESTADO DE GUERRERO

COMPUTER CRIMES: A SUBJECT OF LEGISLATIVE ATTENTION IN THE STATE OF GUERRERO

Dr. Caritino Santiago Morales
Universidad Autónoma de Guerrero, México

Dra Perla Elizabeth Ventura Ramos
Universidad Autónoma de Guerrero, México

Dra. Norma Yadira Memije Alarcón
Universidad Autónoma de Guerrero, México

DOI: https://doi.org/10.37811/cl_rcm.v8i6.15520

Delitos Informáticos: Un Tema de Atención Legislativa en el Estado de Guerrero

Dr. Caritino Santiago Morales[1]
santiagocaritino@gmail.com
https://orcid.org/0009-0006-0412-4547
Universidad Autónoma de Guerrero- Estado de Guerrero - México

Dra Perla Elizabeth Ventura Ramos
ventura-eliza31@hotmail.com
https://orcid.org/0000-0001-8680-1703
Universidad Autónoma de Guerrero- Estado de Guerrero - México

Dra. Norma Yadira Memije Alarcón
normitamemije@hotmail.com
https://orcid.org/0000-0002-3402-1112
Universidad Autónoma de Guerrero- Estado de Guerrero - México

RESUMEN

El presente artículo examina el marco normativo que rige los delitos informáticos en el Estado de Guerrero, México, y la urgente necesidad de actualizar dicha legislación para hacer frente a las nuevas modalidades delictivas asociadas con el uso de tecnologías de la información. Basado en un estudio cualitativo documental, se analiza la legislación actual en Guerrero, comparándola con otros estados y marcos internacionales. El artículo destaca la falta de tipificación penal adecuada y la necesidad de una reforma legislativa integral. Se proponen medidas concretas para que el Estado adopte una normativa que se ajuste a los desafíos contemporáneos de la cibercriminalidad. El texto propone que el estado adopte una reforma legislativa integral que contemple la tipificación específica de delitos informáticos como el acceso no autorizado a sistemas, la revelación de secretos y el uso indebido de datos personales. Además, se enfatiza la importancia de capacitar a las autoridades locales en ciberseguridad y forensía digital, dada la complejidad técnica de estos delitos. El artículo concluye que, sin una reforma legislativa y una estrategia integral de ciberseguridad, Guerrero permanecerá vulnerable a la cibercriminalidad, con consecuencias negativas tanto para los ciudadanos como para las instituciones.

Palabras claves: delitos informáticos, cibercriminalidad, legislación

[1] Autor principal
Correspondencia: santiagocaritino@gmail.com

Computer Crimes: A Subject of Legislative Attention in the State of Guerrero

ABSTRACT

This article examines the regulatory framework governing computer crimes in the State of Guerrero, Mexico, and the urgent need to update such legislation to address new criminal modalities associated with the use of information technologies. Based on a qualitative documentary study, the current legislation in Guerrero is analyzed, comparing it with other states and international frameworks. The article highlights the lack of adequate criminalization and the need for comprehensive legislative reform. Concrete measures are proposed for the state to adopt regulations that meet the contemporary challenges of cybercrime. The text proposes that the state adopt a comprehensive legislative reform that contemplates the specific criminalization of computer crimes such as unauthorized access to systems, disclosure of secrets and misuse of personal data. It also emphasizes the importance of training local authorities in cybersecurity and digital forensics, given the technical complexity of these crimes. The article concludes that without legislative reform and a comprehensive cybersecurity strategy, Guerrero will remain vulnerable to cybercrime, with negative consequences for both citizens and institutions.

Keywords: computer crimes, cybercrime, legislation

Artículo recibido 10 septiembre 2024
Aceptado para publicación: 16 octubre 2024

INTRODUCCIÓN

El Internet es una de las herramientas tecnológicas más utilizadas hoy en día, es la mayor fuente de consulta de información y una de las mayores plataformas comerciales, lo que ha causado que gran número de actividades antijurídicas se realicen a través de este medio.

Los delitos informáticos se refieren a aquellas acciones delictivas cometidas a través del uso de tecnologías de la información y comunicación (TIC), en especial el internet y las computadoras. De acuerdo con la doctrina penal, los delitos informáticos se dividen en dos grandes categorías: aquellos en los que la tecnología es el medio para cometer el delito (por ejemplo, fraude electrónico o estafas en línea) y aquellos en los que la tecnología es el fin del delito (como el hacking o la distribución de software malicioso) (Téllez Valdés, 1996).

El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.

Por lo tanto, es importante partir de una definición clara y una correcta clasificación de estos delitos, ya que, en muchos casos, las legislaciones estatales no han logrado desarrollar un marco penal claro que abarque las diversas formas en que se pueden cometer estas actividades ilícitas (Rodríguez, 2020).

Por su parte encontramos diversos autores y organismos que han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que según éstos se trata de los mismos delitos cometidos a través de otros medios. De hecho, el Código Penal español no contempla los delitos informáticos como tales.

Partiendo de esta compleja situación y tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", encontramos en la Sección 1 del Capítulo II (Derecho penal sustantivo) como:

Los delitos informáticos o los delitos relacionados con el empleo de ordenadores, como los siguientes delitos: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados

con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. (p. 6)

Para Campoli (2002), los delitos informáticos son aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos.

En el contexto iberoamericano, Hikal-Carreón (2013) aborda en su teoría de las Criminologías especializadas la Criminología informática, la cual define como el análisis exhaustivo de la informática (tecnologías electrónicas) y las conductas antisociales que surgen del uso de sistemas electrónicos como medio de comunicación. La Criminología Informática se considera una rama de la Criminología General que se enfoca en el estudio de conductas antisociales y delitos relacionados con el entorno digital. Su objetivo es prevenir y combatir el creciente número de conductas antisociales que se llevan a cabo mediante medios informáticos.

Según nuestro punto de vista es importante reconocer el enfoque preventivo que menciona el autor, ya que de esta forma se pueden prevenir estos delitos, como enfoque consecuente con los propósitos de la criminología como ciencia.

> Plantea Miró (2012) que en los últimos tiempos se ha venido sustituyendo, aunque no por todos, la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al término anglosajón cybercrime, procedente de la unión entre el prefijo cyber, derivado del término cyberspace, y el término crime, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio.

Por su parte Arroyo (2020) refiere que la Criminología, entre una de las conceptualizaciones posibles, puede ser definida como la ciencia empírica, de carácter inter y multidisciplinar holística del fenómeno criminal.

Para el presente estudio se tuvo en cuenta la siguiente metodología

METODOLOGÍA

El presente estudio adopta un enfoque cualitativo basado en el análisis documental de la legislación en materia de delitos informáticos, tanto a nivel federal como estatal. Se revisaron los marcos jurídicos aplicables en México, con un enfoque particular en el Código Penal del Estado de Guerrero. También

se realizó una comparación con la legislación de otros estados mexicanos, como el Estado de México y Baja California, y marcos internacionales para identificar mejores prácticas y propuestas de reforma.

El marco jurídico mexicano frente a los delitos informáticos

El marco normativo vigente en México que regula los delitos informáticos, a pesar de sus esfuerzos, aún necesita, como muchos otros países, de una actualización en esta materia gracia a la velocidad con que se genera la evolución en esta esfera de desarrollo.

La Constitución Política de los Estados Unidos Mexicanos, así como otras leyes federales se encarga de establecer y regular los derechos fundamentales y la protección frente a la manipulación o uso indebido de datos personales y sistemas informáticos. A continuación, se examinan los artículos clave que sustentan la normativa en esta materia, y se aborda cómo las reformas legales recientes han intentado adaptarse a los avances tecnológicos.

Disposiciones constitucionales relevantes

La Constitución Política de los Estados Unidos Mexicanos establece las bases para la regulación de los delitos informáticos, garantizando los derechos a la privacidad, la protección de datos y la seguridad en el ámbito digital.

Artículo 1: Este artículo consagra el respeto a los derechos humanos, entre ellos el derecho a la privacidad y la protección de la información personal. En el contexto de los delitos informáticos, cualquier violación a la privacidad, como el acceso no autorizado a datos personales o la divulgación de información sensible, constituye una transgresión a este principio fundamental (Constitución Política de los Estados Unidos Mexicanos, 2020).

Artículo 6: Establece el derecho a la información y a la libertad de expresión, pero también contempla limitaciones en cuanto al uso de información que pueda afectar los derechos de terceros o comprometer la seguridad pública. Este artículo es especialmente importante en la regulación de la cibercriminalidad, ya que los delitos informáticos a menudo involucran la manipulación de información (Constitución Política de los Estados Unidos Mexicanos, 2020).

Artículo 16: Garantiza el derecho a la inviolabilidad de las comunicaciones privadas y establece que ninguna persona puede ser molestada en sus posesiones, salvo por mandato judicial. Este artículo

sustenta la protección frente a la intervención ilegal en las comunicaciones y los accesos no autorizados a sistemas informáticos (Constitución Política de los Estados Unidos Mexicanos, 2020).

Artículo 73: Otorga al Congreso la facultad de legislar en materia penal, lo que ha permitido que los delitos informáticos sean tipificados en el Código Penal Federal. Este marco legal es clave para regular las conductas ilícitas que se producen en el entorno digital.

Leyes federales aplicables a los delitos informáticos

Entre estas encontramos

Ley Federal del Derecho de Autor: Esta ley ofrece protección a los creadores de programas de computación, regulando la reproducción, distribución y modificación de software sin la autorización del titular de los derechos. La piratería de software es uno de los delitos informáticos más comunes en México, y esta ley establece sanciones específicas para quienes distribuyan o utilicen software sin los permisos correspondientes (Carrillo, 2019).

Ley de Propiedad Industrial: Protege el uso de información confidencial, como los secretos industriales, en el contexto de las actividades comerciales. El robo de datos empresariales o secretos industriales a través de medios informáticos se castiga severamente bajo esta ley, especialmente si la información sustraída afecta la competitividad de una empresa (González, 2020).

Código Penal Federal: Tipificación de delitos informáticos

El Código Penal Federal fue reformado en 1999 para incluir los artículos 211 bis 1 al 211 bis 7, que tipifican diversas conductas delictivas relacionadas con los delitos informáticos. Estos artículos son cruciales en la lucha contra la cibercriminalidad en México, ya que abarcan delitos como el acceso no autorizado a sistemas de información, la destrucción o alteración de datos, y el uso indebido de información almacenada electrónicamente (Hernández, 2023).

Entre las conductas sancionadas se encuentran

Acceso no autorizado a sistemas informáticos: Cualquier persona que, sin el consentimiento del titular, acceda a un sistema informático protegido por algún mecanismo de seguridad, puede ser sancionada. Este tipo de delito es común en casos de hacking, donde los ciberdelincuentes vulneran sistemas de empresas o individuos para obtener información sensible o cometer fraudes (Código Penal Federal, 2020).

Destrucción o modificación de información: Alterar o borrar información contenida en sistemas electrónicos es otro delito tipificado en el Código Penal. Este tipo de delito afecta principalmente a empresas que dependen de la integridad de sus bases de datos para el funcionamiento de sus actividades (García Beltrán, 2000).

Uso indebido de información: La copia o divulgación no autorizada de información contenida en sistemas protegidos también está tipificada como delito. Este tipo de delito se relaciona con el robo de datos personales o información comercial valiosa, como estrategias empresariales o listas de clientes (Código Penal Federal, 2020).

Ley Federal de Transparencia y Acceso a la Información Pública

La Ley Federal de Transparencia y Acceso a la Información Pública establece un marco para garantizar que las instituciones gubernamentales manejen la información de manera segura, especialmente los datos personales de los ciudadanos. Esta ley impone responsabilidades a las entidades públicas para proteger la información sensible contra ataques cibernéticos y usos indebidos. En el contexto de los delitos informáticos, la falta de protección adecuada de la información gubernamental puede dar lugar a sanciones (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, 2021).

Jurisprudencia y avances en la regulación de delitos informáticos

Las decisiones de la Suprema Corte de Justicia de la Nación han sido fundamentales para aclarar cuestiones relacionadas con la responsabilidad de los ciberdelincuentes y la protección de los derechos fundamentales en el entorno digital (SCJN, 2019).

Un ejemplo de esto es la interpretación de los derechos a la privacidad y a la protección de datos personales en el contexto del uso de redes sociales y plataformas digitales. Los tribunales han determinado que la información compartida en estas plataformas está sujeta a los mismos principios de protección que cualquier otro tipo de información, lo que amplía el alcance de las leyes de protección de datos en el entorno digital (SCJN, 2019).

Desafíos en la implementación y armonización de la legislación

Uno de los mayores desafíos encontrados son la falta de armonización entre las leyes federales y las estatales. Aunque el Código Penal Federal establece una base sólida para la tipificación de los delitos

informáticos, muchos estados, como Guerrero, no han adaptado completamente sus normativas para incluir estos tipos penales. Esta falta de uniformidad crea vacíos legales que dificultan la persecución y sanción efectiva de los ciberdelincuentes a nivel local (Santiago Morales et al., 2016).

Otro reto es la rápida evolución de la tecnología, que a menudo deja desactualizadas las leyes existentes. La velocidad a la que surgen nuevas formas de cibercriminalidad exige una constante revisión y actualización de las normativas para que sean efectivas frente a los delitos emergentes.

Por lo tanto, se hace necesario sugerir la necesidad evidente de reformar y fortalecer el marco jurídico a nivel federal y estatal para abordar de manera más efectiva los delitos informáticos, así como para instrumentar estas actualizaciones en los estados de la nación, según sus propias características. Entre las recomendaciones se incluyen:

Actualización constante de las leyes: Las leyes deben ser revisadas regularmente para adaptarse a las nuevas modalidades de cibercriminalidad. Esto incluye tanto la tipificación de nuevos delitos como el ajuste de las penas existentes.

Capacitación de autoridades: Es esencial que las autoridades encargadas de investigar y sancionar los delitos informáticos reciban capacitación especializada en ciberseguridad y forensía digital para poder llevar a cabo investigaciones más eficientes (Ríos Estavillo, 1997).

Cooperación internacional: Dado que muchos delitos informáticos tienen un carácter transnacional, es crucial fortalecer la cooperación con otros países para intercambiar información y estrategias para la persecución de ciberdelincuentes.

Consideramos además que es de vital importancia para la comprensión del tema de los delitos informáticos, área de reciente desarrollo en el derecho penal, considerar los elementos tradicionales del delito, como son: acción, tipicidad, antijuridicidad, culpabilidad e imputabilidad, pero adaptadas a las características particulares de los delitos que se cometen mediante el uso de tecnologías de la información y comunicación (TIC).

Los delitos informáticos abarcan una amplia gama de actividades ilícitas que van desde el acceso no autorizado a sistemas hasta el robo de identidad y la distribución de software malicioso. A continuación, se exponen los elementos del delito que deben ser reexaminados para enfrentar los retos que plantea el entorno digital.

Elementos del Delito Aplicados a los Delitos Informáticos

En el análisis de los delitos informáticos, los elementos clásicos del delito se conservan, aunque adaptados a las nuevas modalidades delictivas digitales. A continuación, se detallan estos elementos:

Acción: En los delitos informáticos, la acción consiste generalmente en la intervención ilícita en un sistema informático o en datos electrónicos. Puede incluir actos como el acceso no autorizado a una red, la destrucción de información o la creación de virus informáticos. A diferencia de otros delitos tradicionales, la acción en el ámbito digital a menudo se lleva a cabo de manera remota y anónima, lo que dificulta la identificación y persecución de los responsables (Téllez Valdés, 1996).

Tipicidad: Para que una conducta sea considerada delictiva, debe estar descrita en la ley penal. Los delitos informáticos, como el hacking o el phishing, no estaban originalmente contemplados en los códigos penales tradicionales, por lo que fue necesario que los legisladores introdujeran reformas para tipificar estas conductas. En México, el Código Penal Federal ahora incluye delitos como el acceso no autorizado a sistemas informáticos y la alteración de datos electrónicos (García Beltrán, 2000).

Antijuridicidad: Este elemento implica que la conducta debe ser contraria a derecho. En el caso de los delitos informáticos, la antijuridicidad puede encontrarse en el uso indebido de sistemas o información sin el consentimiento de sus titulares. La violación de la privacidad, por ejemplo, es una conducta antijurídica si se realiza mediante el acceso no autorizado a correos electrónicos o redes sociales (Rodríguez, 2020).

Culpabilidad: La culpabilidad se refiere a la capacidad del delincuente para entender y responsabilizarse de sus acciones. En los delitos informáticos, esto plantea preguntas sobre el conocimiento especializado necesario para cometer ciertos tipos de delitos, como la creación de malware o la ejecución de ataques de denegación de servicio (DDoS). El nivel de conocimiento técnico del delincuente puede influir en la pena que se le imponga (Ríos Estavillo, 1997).

Imputabilidad: Este elemento evalúa si el autor del delito tenía la capacidad mental para comprender la ilicitud de su acción. En el ámbito de los delitos informáticos, esto puede ser un área controvertida, especialmente en casos donde los autores son menores de edad o personas con trastornos mentales que utilizan la tecnología sin plena conciencia de las consecuencias legales de sus actos.

Clasificación de los Delitos Informáticos

Esta clasificación es esencial para la correcta tipificación y sanción de las conductas delictivas en el entorno digital.

Delitos en los que la informática es el medio: En estos casos, la tecnología es utilizada como herramienta para cometer delitos tradicionales, como el fraude o la extorsión. El fraude electrónico es un ejemplo clásico, donde se utilizan correos electrónicos o sitios web falsos para obtener información confidencial de las víctimas. En este tipo de delito, la tecnología facilita la comisión del ilícito, pero el objeto sigue siendo el mismo que en un delito tradicional (González, 2018).

Delitos en los que la informática es el fin: Aquí, la tecnología no es solo un medio, sino el objetivo principal del delito. Ejemplos incluyen el hacking, donde el delincuente busca acceder a sistemas informáticos para alterar o destruir información, o el robo de identidad digital, en el que el atacante sustrae datos personales de una víctima para utilizarlos fraudulentamente. Estos delitos son característicos del ciberespacio y requieren un conocimiento técnico especializado para su comisión (Carrillo, 2019).

Características Específicas de los Delitos Informáticos

Los delitos informáticos presentan características que los diferencian significativamente de los delitos tradicionales:

Transnacionalidad: Muchos delitos informáticos tienen un alcance internacional, lo que dificulta su persecución y sanción. Un ciberdelincuente puede operar desde cualquier lugar del mundo, lo que complica la competencia territorial de las autoridades judiciales. La Interpol ha señalado que la colaboración entre países es crucial para enfrentar el crecimiento de la cibercriminalidad (Interpol, 2020).

Anonimato: Una característica importante de los delitos informáticos es el alto grado de anonimato que permite el uso de redes como la dark web. Los delincuentes pueden ocultar su identidad mediante el uso de redes privadas virtuales (VPN) y técnicas de cifrado, lo que les permite actuar sin dejar rastros evidentes (Gómez, 2020).

Velocidad y automatización: Los delitos informáticos pueden ejecutarse a una velocidad mucho mayor que los delitos tradicionales. Un ataque de phishing o la distribución de un virus informático puede

afectar a miles de víctimas en cuestión de minutos. Esta capacidad de propagación rápida es una de las mayores preocupaciones de las autoridades de ciberseguridad a nivel mundial (López de la Peña, 2021).

Desafíos Jurídicos y Tecnológicos en la Persecución de los Delitos Informáticos

Es importante analizar los retos que enfrenta el derecho penal en la investigación y sanción de los delitos informáticos. Uno de los mayores desafíos es la falta de pruebas físicas. A diferencia de los delitos tradicionales, los delitos informáticos no dejan huellas tangibles, lo que complica la recolección de evidencia.

Además, los mecanismos tradicionales de investigación no siempre son aplicables en el entorno digital. La persecución de los ciberdelitos requiere el uso de herramientas avanzadas de análisis forense digital, lo que implica la necesidad de capacitar a las fuerzas del orden y al personal judicial en ciberseguridad y tecnología informática.

Por otro lado, la rapidez de los avances tecnológicos genera una brecha entre las normativas vigentes y las nuevas modalidades delictivas. Por ejemplo, la aparición de nuevas tecnologías, como la inteligencia artificial o el internet de las cosas (IoT), ha abierto la puerta a nuevos tipos de delitos que aún no están contemplados en la legislación penal (Rodríguez, 2020).

Por estas razones consideramos ofrecer una propuesta de Reforma y Medidas Preventivas para mejorar la regulación de los delitos informáticos en México:

Reforma legislativa: Se propone una actualización constante del Código Penal Federal y de las leyes locales para que incluyan las nuevas formas de cibercriminalidad que surgen con los avances tecnológicos. Esto incluye la tipificación de delitos relacionados con la inteligencia artificial y el internet de las cosas.

Capacitación y formación de autoridades: Es esencial que las autoridades encargadas de la investigación y persecución de delitos informáticos reciban capacitación continua en ciberseguridad y forensía digital. La complejidad técnica de estos delitos exige que el personal esté bien preparado para enfrentarlos.

Concientización ciudadana: Las campañas de educación pública sobre los riesgos de los delitos informáticos y las medidas de seguridad que los usuarios pueden adoptar son fundamentales para prevenir la cibercriminalidad. Esto incluye la enseñanza sobre cómo proteger la información personal y financiera en línea y cómo identificar correos electrónicos o sitios web sospechosos (Gómez, 2020).

Delitos Informáticos en el Estado de Guerrero

El fenómeno de los delitos informáticos ha crecido a nivel global y México no es la excepción. El estado de Guerrero, ubicado en el suroeste del país, enfrenta graves problemas en cuanto a la cibercriminalidad, exacerbados por la falta de una infraestructura tecnológica avanzada y de una legislación adecuada. Si bien el uso de tecnologías de la información ha avanzado en Guerrero, este progreso también ha traído consigo el incremento de los delitos cometidos mediante medios digitales.

Los principales problemas derivados de esta situación son la falta de una tipificación clara de estos delitos en el Código Penal del Estado de Guerrero y las limitaciones en la persecución de los cibercriminales debido a la escasa capacitación de las autoridades locales (Santiago Morales et al., 2016).

Los delitos informáticos en Guerrero comprenden desde el fraude electrónico y el robo de identidad hasta actividades más sofisticadas como el hacking y la distribución de software malicioso. Estas actividades ilícitas, si bien no son nuevas, se han intensificado debido a la mayor conectividad de los ciudadanos y empresas de la región. La falta de una legislación actualizada ha provocado que muchos de estos delitos no sean denunciados ni perseguidos adecuadamente, generando una sensación de impunidad y vulnerabilidad entre la población (Rodríguez, 2020).

Comparativa con Otros Estados de México

Al comparar la legislación de Guerrero con la de otros estados, como el Estado de México y Baja California, es evidente que Guerrero se encuentra rezagado en la adopción de normas que aborden la cibercriminalidad de manera efectiva. En el Estado de México, por ejemplo, se ha avanzado en la tipificación de delitos como el robo de identidad y el fraude en línea, lo que ha facilitado la labor de las autoridades en la persecución de estos crímenes (González, 2018).

Tipología de los Delitos Informáticos en Guerrero

A continuación, veremos una tipología detallada de las principales formas de cibercriminalidad que afectan al estado:

Fraude Electrónico: Este es uno de los delitos informáticos más comunes en Guerrero. Los ciberdelincuentes utilizan correos electrónicos falsos, sitios web fraudulentos o mensajes de texto para engañar a las víctimas y obtener información confidencial, como contraseñas o números de tarjetas de

crédito. Este tipo de fraude suele derivar en robo de identidad o en transacciones fraudulentas que afectan a las víctimas tanto económicamente como psicológicamente (González, 2018).

Robo de Identidad: El robo de identidad digital es otro delito que ha crecido significativamente en Guerrero. A través de técnicas como el phishing y el smishing, los delincuentes logran obtener los datos personales de las víctimas, que luego utilizan para realizar compras, obtener préstamos o cometer otros fraudes en su nombre. La falta de protección de datos personales en los sistemas gubernamentales y privados en Guerrero facilita la comisión de este tipo de delitos (Gómez, 2020).

Acceso No Autorizado a Sistemas Informáticos: El acceso no autorizado, comúnmente conocido como hacking, consiste en vulnerar la seguridad de sistemas informáticos para acceder a información que no está disponible públicamente. En Guerrero, tanto empresas privadas como instituciones gubernamentales han sido víctimas de este delito, lo que ha comprometido la seguridad de datos sensibles. La falta de infraestructura tecnológica avanzada y de personal especializado en ciberseguridad en la región agrava este problema (Carrillo, 2019).

Extorsión Cibernética: La extorsión cibernética es un delito en el que los delincuentes amenazan con divulgar información comprometedora o con llevar a cabo ataques a los sistemas de la víctima a menos que se les pague una cantidad de dinero. Este tipo de extorsión afecta tanto a individuos como a empresas en Guerrero, y su anonimato en la web hace que sea difícil rastrear a los responsables (Interpol, 2020).

La Legislación Estatal y su Insuficiencia

El Código Penal del Estado de Guerrero no cuenta con una regulación específica para los delitos informáticos, lo que ha resultado en una considerable brecha jurídica. A diferencia de otros estados de México, Guerrero no ha adoptado las reformas necesarias para tipificar estos delitos y sancionarlos adecuadamente. Aunque a nivel federal existen disposiciones en el Código Penal Federal que regulan algunos aspectos de la cibercriminalidad, a nivel estatal la falta de una legislación moderna impide que las autoridades locales actúen eficazmente contra los ciberdelincuentes (Santiago Morales et al., 2016).

Esta insuficiencia legislativa se refleja en la incapacidad de las autoridades para procesar adecuadamente los casos relacionados con cibercrímenes. Las denuncias relacionadas con fraudes electrónicos, por ejemplo, muchas veces no son investigadas debido a que no se encuentran tipificadas de manera clara

en las leyes estatales. Esto genera una sensación de impunidad entre los ciberdelincuentes, que explotan las lagunas jurídicas existentes en Guerrero para operar sin mayores restricciones (Rodríguez, 2020).

Retos en la Persecución de los Delitos Informáticos en Guerrero

Uno de los mayores obstáculos para enfrentar los delitos informáticos en Guerrero es la falta de capacitación especializada de las autoridades locales. La Policía Cibernética, una unidad esencial para la investigación de estos delitos, no cuenta con los recursos necesarios ni con personal altamente capacitado en el estado. Esto limita su capacidad para investigar casos de cibercriminalidad, rastrear a los responsables y reunir pruebas digitales que sean admisibles en un tribunal (García Beltrán, 2000).

Además, las limitaciones tecnológicas son otro desafío significativo. Las instituciones judiciales y las fuerzas del orden en Guerrero no disponen de las herramientas tecnológicas avanzadas necesarias para realizar investigaciones forenses digitales, lo que dificulta la obtención de pruebas. En muchos casos, las investigaciones dependen del apoyo de autoridades federales o de otras entidades con mayor capacidad tecnológica, lo que retrasa las resoluciones y afecta la eficacia de la justicia (López de la Peña, 2021).

Otro reto es la colaboración insuficiente entre las autoridades locales y las federales. Dado que muchos delitos informáticos tienen un carácter transnacional, es esencial que exista una cooperación más estrecha entre las entidades estatales, federales e incluso internacionales. La falta de un sistema integral de intercambio de información entre las diferentes jurisdicciones dificulta la lucha contra la cibercriminalidad en Guerrero (Interpol, 2020).

Propuestas para la Mejora del Marco Legal y Operativo

Propuestas para mejorar la situación jurídica y operativa en torno a los delitos informáticos en Guerrero: Reforma del Código Penal del Estado de Guerrero: Es fundamental que se lleve a cabo una reforma legislativa que contemple la tipificación clara y detallada de los delitos informáticos. Esto incluiría la creación de artículos específicos que regulen el acceso no autorizado a sistemas informáticos, el robo de identidad digital, la extorsión cibernética y la distribución de malware (Gómez, 2020).

Capacitación de las Autoridades: Es necesario que las fuerzas del orden y los funcionarios judiciales reciban capacitación continua en ciberseguridad y forensía digital. Esto mejoraría su capacidad para investigar delitos informáticos y para presentar pruebas digitales en los tribunales.

Desarrollo de Unidades Especializadas: La creación de una unidad especializada en cibercrímenes dentro de la policía estatal es crucial. Esta unidad estaría dedicada exclusivamente a la investigación y persecución de delitos cibernéticos, contando con personal capacitado y las herramientas tecnológicas necesarias para enfrentar este tipo de delitos.

Mejora en la Colaboración Federal y Estatal: Guerrero debe fortalecer su cooperación con las autoridades federales, particularmente con la Policía Cibernética Nacional y la Guardia Nacional, para garantizar que los delitos con implicaciones federales o transnacionales sean investigados y procesados de manera adecuada (Rodríguez, 2020).

Prevención y Concientización Pública: Además de las reformas legislativas y operativas, es necesario subrayar la importancia de concientizar a la ciudadanía sobre los riesgos de los delitos informáticos. La implementación de campañas educativas dirigidas tanto a ciudadanos como a empresas es esencial para reducir la vulnerabilidad frente a los ciberdelincuentes. Estas campañas deberían enfocarse en enseñar a las personas cómo proteger su información personal y financiera, cómo identificar correos electrónicos fraudulentos y cómo evitar caer en estafas en línea (Gómez, 2020).

CONCLUSIÓN

El análisis de los delitos informáticos en el estado de Guerrero revela una problemática compleja que requiere la atención urgente de las autoridades locales. La falta de una legislación adecuada, combinada con la escasa capacitación y los recursos limitados, ha permitido que la cibercriminalidad crezca sin control en la región. Es imperativo que se implementen reformas legislativas que tipifiquen claramente los delitos informáticos, y que se capacite a las autoridades para enfrentar los desafíos que presenta este tipo de criminalidad. Además, la concientización ciudadana y la cooperación entre los niveles estatal y federal son fundamentales para proteger a la población de los riesgos del entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Cámara, S. (2020) Estudios criminológicos contemporáneos (IX): La cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social N.° 60, ABR-JUN 2020. Recuperado de: https://www.bing.com/search?q=Hikal-Carre%C3%B3n+%282013%29+teor%C3%ADa+de+las+Criminolog

Campoli, G. A. (2002). Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos. AR. Derechos Informáticos, núm 048.

Carrillo, M. (2019). El marco legal de los delitos informáticos en México: Análisis comparado. Revista de Derecho Penal, 45(2), 65-89.

Código Penal del Estado de Guerrero (2017) Recuperado de: http://tsjguerrero.gob.mx/transparencia/instituto_mejoramiento_judicial/2017/Octubre/Codigo_Penal_para_el_Estado_de_Libre_y_Soberano_de_Guerrero.pdf

Código Penal Federal. (2020). México: Cámara de Diputados del H. Congreso de la Unión.

Constitución Política de los Estados Unidos Mexicanos. (2020). México: Congreso de la Unión.

Convenio sobre la Ciberdelincuencia (STE núm. 185) Recuperado de: https://rm.coe.int/16802fa403

FERNANDO MIRÓ LLINARES (2012) EL CIBERCRIMEN Fenomenología y criminología de la delincuencia en el ciberespacio. Recuperado de: https://www.academia.edu/7865754/El_Cibercrimen_Fenomenolog%C3%ADa_y_criminolog%C3%ADa_de_la_delincuencia_en_el_ciberespacio

García Beltrán, A. (2000). Breve historia de la informática. División de Informática Industrial.

Gómez, J. (2020). El anonimato en la dark web: Implicaciones para la ciberseguridad. Editorial Jurídica Porrúa.

González, A. (2018). Cibercriminalidad en México: Tipificación y retos legales. Gaceta Jurídica, 34(1), 123-139.

González, A. (2020). Propiedad intelectual y derecho digital en México. Editorial Jurídica Porrúa.

Hernández, J, M. (2023) Delitos informáticos, análisis del artículo 211 bis 1 del Código Penal Federal. Tesis para el grado de Licenciado en Derecho. Universidad Nacional Autónoma de México. Facultad de Estudios superiores Aragón. Recuperado de: https://ru.dgb.unam.mx/bitstream/20.500.14330/TES01000849402/3/0849402.pdf

HIKAL-CARREÓN, W.S. (2013). “La especialización de la criminología: De lo general a lo específico, ¿hacía una neocriminología? teoría de las criminologías específicas”, en Derecho y Cambio Social, Año 10, Nº. 32, edición online.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2021). Informe anual sobre protección de datos personales. México.

Interpol. (2020). Informe anual sobre cibercrimen. Recuperado de https://www.interpol.int/cibercrimen

López de la Peña, R. (2021). La velocidad y el anonimato en los delitos informáticos. Editorial Tirant lo Blanch.

Ríos Estavillo, J. J. (1997). Derecho e informática en México. Instituto de Investigaciones Jurídicas.

Rodríguez, P. (2020). Los desafíos de la regulación de delitos informáticos en México. Editorial Porrúa.

Santiago Morales, C., Ventura Ramos, P., Mendoza Urbano, H., & Memije Alarcón, N. (2016). Delitos Informáticos en el Estado de Guerrero. Universidad Autónoma de Guerrero.

Suprema Corte de Justicia de la Nación (SCJN). (2019). Jurisprudencia y criterios sobre protección de datos personales. México.

Téllez Valdés, J. (1996). Derecho informático. 2ª. ed. México, Editorial, McGraw-hill,1996, p.7