VOL. 05, NO. 02, JULIO-DICIEMBRE, PP. 354-386, 2025

# FUNDAMENTOS CRIMINOLÓGICOS PARA EL ANÁLISIS DE LA CIBERDELINCUENCIA PATRIMONIAL CONTRA PERSONAS NATURALES EN CUBA

## Criminological foundations for the analysis of property cybercrime against individuals in Cuba

**M.Sc. Camila María González Font**

Profesora Asistente de Derecho Penal
Universidad de La Habana (Cuba)
https://orcid.org/0000-0001-8847-8540
camila.gonzalez@lex.uh.cu

***Resumen***

Con la apertura de Cuba a Internet, la nación y los usuarios de las redes se han enfrentado con una de las más nocivas prácticas del uso de las TIC. Cuba se encuentra expuesta hoy a los ciberdelitos en un contexto complejo para su prevención y enfrentamiento. Se hace necesario, en este sentido, proyectar estrategias de prevención y reforzar los mecanismos y las herramientas investigativas y forenses para el enfrentamiento a esta nueva forma de delincuencia, a la que ya se le ha identificado en el mundo como "delincuencia emergente". Específicamente, la ciberdelincuencia patrimonial es una de las expresiones más comunes de ciberdelincuencia en la Cuba de hoy. El presente artículo científico persigue como objetivo determinar y analizar los fundamentos criminológicos para el abordaje de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba, para de esta forma contribuir a la prevención del fenómeno, partiendo del entendido de que la criminología y el Derecho como ciencias sociales no pueden apartar los ojos ante esta realidad. Las manifestaciones de ciberdelincuencia son cada día más visibles y comunes, y su castigo se torna difícil. Se trata de un objeto investigativo que se encuentra dentro del campo de estudio de la criminología, pues se trata de una nueva forma de delincuencia, y de un tipo de delincuente que al advertir nichos favorables para su conducta criminal ocasiona graves perjuicios, lo que constituye hoy, sin dudas, una real amenaza social y económica para Cuba.

**Palabras claves:** fundamentos criminológicos; abordaje; ciberdelincuencia patrimonial.

***Abstract***

With Cuba's opening to the internet, the nation and network users have encountered one of the most harmful practices in the use of ICT. Cuba is today exposed to cybercrimes in a complex context for its prevention and confrontation. In this sense, it is necessary to project prevention strategies and reinforce investigative and forensic mechanisms and tools to confront this new form of crime, which has already been identified in the world as "emerging crime." Specifically, property cybercrime is one of the most common expressions of cybercrime in Cuba today. The objective of this scientific article is to determine and analyze the criminological foundations for addressing property cybercrime that affects natural persons in Cuba, in order to contribute to the prevention of the phenomenon, based on the understanding that Criminology and Law as Social Sciences cannot turn their eyes away from this reality. The manifestations of cybercrime are becoming more visible and common every day, and their punishment becomes difficult. It is an investigative object that is within the field of study of Criminology, since it is a new form of crime, and a type of criminal who, noticing favorable niches for his criminal behavior, causes serious damage, which that constitute today, without a doubt, a real social and economic threat for Cuba.

**Keywords:** criminological foundations; approach; property cybercrime.

***Sumario***



## 1. A MODO DE INTRODUCCIÓN

Es la aparición de las Tecnologías de la Información y las Comunicaciones (TIC), pero sobre todo su masificación, el elemento que mejor define la nueva era que se vive. Si algo ha revolucionado la sociedad es Internet, gran invento del siglo XX y símbolo de la época actual. Internet ha facilitado las relaciones sociales, y en

general toda comunicación e intercambio de información. Las estadísticas arrojan un imparable y progresivo crecimiento de las personas que acceden habitualmente a Internet año tras año. Esto sin duda prueba su consolidación como elemento comunicativo, comercial o de ocio.[1]

La evolución hacia la sociedad de la información ha supuesto una transformación profunda de las relaciones sociales, y uno de los efectos de este proceso ha sido la transformación de la delincuencia.[2] La incorporación masiva de las TIC y en particular de las redes telemáticas, principalmente Internet como red abierta, a la vida cotidiana y su fácil accesibilidad por cualquier persona, han provocado un nuevo giro y nuevas manifestaciones de la criminalidad cibernética, donde han sido insuficientes las respuestas jurídicas con el fin de prevenir o sancionar su desarrollo.[3]

Según datos de la Oficina Nacional de Estadísticas e Información (ONEI) al cierre de 2021, tenían acceso a internet en Cuba 7,5 millones, lo que representa el 68 % de la población del país.[4] Estas cifras son contrastables con las del año 2011, donde solo el 16 % de la población tenía acceso a Internet. Ello demuestra que las tecnologías han irrumpido de forma rápida, trayendo consigo, además de sus nobles ventajas, numerosos riesgos que ponen en peligro desde la seguridad de una nación hasta el patrimonio de sus ciudadanos.

Con la apertura de nuestro país a internet, los usuarios de las redes se han enfrentado con una de las más nocivas prácticas del uso de las Tecnologías de la Información y las Comunicaciones. La nación se encuentra expuesta hoy, como nunca antes, a los ciberdelitos en un contexto desfavorable, toda vez que no están demostrando ser eficaces las herramientas jurídicas y criminológicas para el correcto abordaje de la prevención y el enfrentamiento a esta nueva

---

1 Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución. El Convenio de Budapest", *Revista Electrónica de Derecho de La Universidad de la Rioja (REDUR*), No. 8, 2010, p. 171.

2 Tamarit Sumalla, Josep, "Ciberdelincuencia y victimización", *Revista de Internet Derecho y Política*, No. 22, 2016.

3 Romeo Casabona, Carlos María e Iñigo de Miguel Beriain, *El cibercrimen económico y patrimonial. Guía Docente*, p. iii.

4 *Juventud Rebelde*, Diario de la Juventud cubana, "Más de 7,5 millones de cubanos con internet", 17/6/2022.

forma de delincuencia, a la que ya se le ha identificado en el mundo como "delincuencia emergente".[5]

Las manifestaciones de ciberdelincuencia en Cuba se han incrementado de manera considerable, debido a la informatización de la sociedad, con el incremento del uso de las redes sociales, la tecnología, el uso de la telefonía celular, el acceso de mayor cantidad de personas al comercio electrónico, las transacciones comerciales y la apertura a un mundo digital, en un contexto favorable para su crecimiento y auge, y desfavorable para los usuarios de las redes. Desde la apertura de Cuba a Internet, con un auge significativo en el periodo de la Covid-19, hubo quienes, aprovechando sus conocimientos informáticos, advirtieron brechas y comenzaron a realizar actos con el objetivo de enriquecer su patrimonio personal en detrimento del ajeno, empleando para estos actos delictivos, la tecnología de la informática y las comunicaciones. Las estafas informáticas y el robo con fuerza en las cosas han cobrado especial auge, siendo numerosas las víctimas y relevantes los daños patrimoniales causados a la economía de estas.[6]

La ciberdelincuencia patrimonial, como una de las expresiones de la ciberdelincuencia consistente en la obtención de un enriquecimiento patrimonial en perjuicio de un tercero valiéndose de un sistema informático, goza hoy de ventaja sobre quienes intentan ponerles freno a estas manifestaciones. Esta supone un tipo de criminalidad característica y especial con matices particulares que deben ser analizados y tenidos en cuenta para proyectar correcta y eficazmente una estrategia para su prevención. Es por ello que este estudio se propone identificar y analizar los presupuestos criminológicos que permiten abordar el fenómeno en aras de su prevención. Para el logro de este objetivo se

---

5 *Vid.* Secretaría de Naciones Unidas, "Enfoques amplios y equilibrados para prevenir y afrontar adecuadamente formas nuevas y emergentes de delincuencia transnacional", 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Doha, 12 a 19 de abril de 2015.

6 NA: frecuentemente, los sitios oficiales de noticias en Cuba, dígase el órgano oficial del Partido Comunista de Cuba (PCC), periódico *Granma*, *Cubadebate* y el propio Noticiero de Televisión, han informado de continuas estafas informáticas y hurtos mediante las plataformas de EnZona y Transfermóvil, plataformas creadas para el pago electrónico. "Durante 2021 se incrementaron los reportes de defraudaciones a usuarios que emplean las plataformas de pago digital, en los que resulta una vulnerabilidad el desconocimiento de la población en materia de seguridad y protección de sus credenciales y contraseñas, cuando el país avanza en el desarrollo del comercio electrónico". *Vid. Cubadebate*, "Cuba contra el delito: Detenidos autores de defraudaciones en plataformas de pago digitales".

estudiaron expedientes de fase preparatoria trabajados por las divisiones de investigación criminal, la Fiscalía General de la República y la Fiscalía Provincial de La Habana, se realizaron encuestas a usuarios de las redes y entrevistas a especialistas en la materia en la profesión de magistrados, fiscales, investigadores y expertos en ciberseguridad.

## 2. ACERCAMIENTO JURÍDICO, DOCTRINAL Y CRIMINOLÓGICO A LA CIBERDELINCUENCIA

La introducción de las TIC en la vida cotidiana ha dado lugar al desarrollo del moderno concepto de sociedad de la información. Los desarrollos técnicos han impactado de forma directa en la vida diaria, alcanzando un enorme grado de integración de las TIC en nuestras vidas diarias. La enorme expansión que viene gozando el procesamiento automatizado de datos en una sociedad cada vez más receptiva a las posibilidades crecientes que ofrecen los medios informáticos, como bien afirma Mata y Martín, tiene consecuencias indudables para el mundo del Derecho.[7]

Este desarrollo de la sociedad de la información ofrece grandes ventajas, como son la simplificación de procesos cotidianos y organizacionales que tienen un impacto en la calidad de vida y la evolución social; el mayor acceso a la información; facilita la interacción y comunicación entre individuos; la transferencia de conocimiento en todo el mundo; facilita el acceso a la educación y al trabajo; genera nuevos empleos, dando la posibilidad de modalidades de trabajo que no requieren la presencia de los empleados; así mismo genera oportunidades de negocios, posibilitando el crecimiento económico, a la vez que permite optimizar los trámites burocráticos. Sin embargo, el crecimiento de la sociedad de la información viene acompañado de nuevas e importantes amenazas producto de la aparición de nuevas conductas delictivas y de una mayor facilidad para cometer delitos convencionales, surgiendo así la ciberdelincuencia. Esta otra cara de la moneda deja al descubierto la aparición de un nuevo factor criminógeno.

El mundo vive una época de digitalización, peligrosa hasta cierto punto; todos los centros operacionales funcionan y son dirigidos por medio de las tecnologías. La tendencia indica que cada vez se emplea más tiempo en navegar por

[7] Mata y Martín, Ricardo, *Delincuencia informática y Derecho Penal*, p. 21.

la red y, en consecuencia, se trasladan más parcelas de la vida al mundo virtual. Esto se traduce en que cada vez introducimos más valores personales en el ciberespacio, lo que permite a los ciberdelincuentes tener disponibles cada vez más bienes jurídicos para su lesión o puesta en peligro.[8] Este desplazamiento de las oportunidades al ciberespacio, fruto del mayor tiempo y más actividades realizadas en Internet, se traduce necesariamente en un aumento de los ciberdelitos.[9] La cuestión más preocupante es la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente y constante cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a estas.

La ciberdelincuencia en sentido amplio concibe como ciberdelito a aquel comportamiento delictivo realizado en el ciberespacio, entendiendo además este al ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet. Por el contrario, la ciberdelincuencia en sentido restringido admite como ciberdelito únicamente al comportamiento delictivo realizado en el ciberespacio, cuya esencia de injusto no podría haberse dado de ninguna otra manera fuera de él.

Es el sentido amplio de la ciberdelincuencia el que se desarrolla en este estudio. La ciberdelincuencia como categoría criminológica engloba los ciberdelitos,[10] que no solo son aquellos delitos que atacan la informática, su integridad, sistema y datos, sino aquellos que, empleando medios informáticos, dañan los

---

8 López Gorostidi, Jon, "Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia", *Revista chilena de Derecho y Tecnología*, Vol. 11, No. 1, p. 122.

9 Miró Llinares, Fernando, "Crimen, cibercrimen y COVID-19, Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", *Revista de Internet, derecho y política*, No. 32, 2021, p. 4.

10 Se considera ciberdelito a aquella acción típica y antijurídica que es cometida mediante las TIC, atentando a la disponibilidad, integridad y confidencialidad de los sistemas informáticos, de las redes, de los datos y derechos de terceros, o haciendo un uso fraudulento de ellos. El ciberdelito comprende todas aquellas conductas en las que las TIC son el objetivo o el medio de ejecución del delito, aunque afecten bienes jurídicos diversos.

bienes jurídicos tradicionalmente protegidos como el patrimonio, la indemnidad sexual, el honor, entre otros.

Con respecto al bien jurídico protegido, se puede afirmar que los ciberdelitos no solo dañan en su comisión bienes jurídicos propiamente informáticos, sino que su objeto de protección coincide con el de los tipos tradicionales que están siendo adaptados a las nuevas tecnologías, a la vez que pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos, de las redes de transmisión de datos y la integridad de los sistemas informáticos, telecomunicaciones, las tecnologías de la información y la comunicación y sus servicios. La gravedad de este quebrantamiento de confianza radica, precisamente, en la dependencia de la sociedad actual respecto de las TIC para el desarrollo personal, económico y social de los individuos.

Una de las clasificaciones en la doctrina es la que cataloga los ciberdelitos en delitos cibereconómicos o patrimoniales, que son los que afectan al patrimonio de sus víctimas; los delitos ciberintrusivos, que son los que dañan la esfera más personal de los ciudadanos, ya que son los relativos a bienes jurídicos personalísimos como la intimidad, la libertad, la libertad sexual o el honor; y los delitos de ciberterrorismo, que afectan a la paz pública.[11] Otra de las clasificaciones más extendidas es aquella introducida por Miró Llinares,[12] la cual clasifica los ciberdelitos en:

a) Puros, donde las tecnologías de la información y la comunicación son el medio de comisión del ciberdelito y el objetivo de él. Aquí se encuentran el *hacking* (acceso ilícito a sistemas informáticos), *cracking*, infecciones de *malware* (software malicioso que busca dañar o explotar dispositivos o redes informáticas) y otras formas de sabotaje cibernético.

[11] López Gorostidi, Jon. "Sobre el alcance...", *cit.*, p. 128.

[12] *Vid.* Miró Llinares, Fernando, *El cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio*, p. 50.

b) De réplica, donde la red constituye el medio de ataque a bienes jurídicos tradicionales. En este grupo entran los ciberfraudes (ciberfraudes burdos o *scam*;[13] el *phishing;*[14] *cyberbullying;*[15] *cyberstalking;*[16] ciberespionaje).

c) De contenido, donde el núcleo del injusto está en el material que se divulga por el ciberespacio. En este grupo se destacan la ciberpiratería intelectual, la pornografía infantil, la difusión de otros contenidos ilícitos, como pudiera ser el odio racial.

Además de estos criterios clasificatorios, según el autor *supra* citado, pudiera hablarse de otro criterio relacionado con el sujeto que realiza el delito y su objetivo último. En razón de esto existen aquellos ataques cuyo propósito último es la obtención de un beneficio patrimonial (cibercrimen económico o patrimonial), otros en los que el objeto de ataque es una persona individual (cibercrimen social), en cualquiera de los aspectos de su desarrollo personal, y un tercer grupo de comportamientos de cibercriminalidad en los que no existe ni un propósito económico ni un conflicto vinculado con una relación social, sino un objetivo ideológico o institucional (cibercrimen político).

Al ser el fenómeno de la ciberdelincuencia un fenómeno de reciente aparición, la criminología como ciencia que explica el fenómeno criminal, ha explicado la etiología del cibercrimen desde las diferentes aproximaciones teóricas clási-

---

[13] Correo electrónico masivo no solicitado. Tiene diversas finalidades que van desde el envío ilícito de publicidad, hasta el intento de infección del sistema por medio de malware.

[14] Es un engaño cibernético que busca robar datos sensibles de las víctimas, haciéndose pasar por entidades legítimas. Se utiliza la identidad personal de otro mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivos. Se puede llevar a cabo de muy distintas formas, generalmente, el modo de proceder consiste en la búsqueda de vulnerabilidades en los sistemas informáticos derivadas de una deficiente programación, de un cambio tecnológico que hace obsoleta la formulación binaria existente, o incluso, en la búsqueda y el uso de las puertas que involuntariamente el propio titular del sistema informático o cualquiera de los múltiples sujetos que interaccionan con él pueden haber dejado abiertas.

[15] Variante del ciberacoso en la que un menor atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil o alguna otra tecnología telemática de comunicación.

[16] Es el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien.

cas, al ser estas una explicación unívoca a la génesis de cualquier tipo de delincuencia. Entre estas destacan:

a) La Teoría de la Elección Racional de Clark y Cornish.[17] Esta teoría hace referencia a la elección de un sujeto para delinquir o no. La comisión del delito es fruto de un ejercicio de deliberación de costes y beneficios.

b) La Teoría del Control Social, de los vínculos sociales y del autocontrol fue elaborada por el sociólogo y criminólogo estadounidense Travis Hirschi, quien reconoce que el delito se produce cuando falla el control social y la persona se siente desconectada o no influenciada por el medio, por lo que no tiene que preocuparse sobre la respuesta que tendrán los otros o sobre el daño que le pueda causar a la sociedad.

c) La Teoría de las Actividades Cotidianas/Rutinarias, defendida por Cohen y Felson, que concibe tres factores fundamentales que favorecen la conducta criminal: un ofensor motivado, víctimas propicias y la ausencia de guardianes capaces de actuar contra una vulneración de la norma. Esta teoría explica de forma muy efectiva la ciberdelincuencia, en primer lugar por el anonimato del comisor de este delito, las brechas de seguridad, la ignorancia o el desconocimiento de las víctimas, la falta de eficientes mecanismos de seguridad que constituyen motivaciones para el ciberdelincuente para llevar a su fin el ánimo delictivo, a la vez que reflejan las víctimas propicias y la ausencia de mecanismos efectivos que impidan consumar su finalidad.

d) La Teoría de la Oportunidad de los sociólogos norteamericanos Cloward y Ohlin. Esta teoría explica el delito desde las facilidades para cometerlo, tanto desde el exterior como desde el interior. Estos autores consideraban que lo que explica la desviación es la oportunidad que el sujeto tiene de desviarse.[18]

Otras teorías, sin embargo, parten de una nueva premisa desarrollada específicamente para la explicación del ciberdelito. Es el caso de la Teoría de la Transición Espacial de Jaishankar, que pretende dar una explicación sobre la naturaleza del

---

[17] Patiño Ortega, María, "Teoría de la elección racional de Cornish y Clarke", *Revista Crimipedia*, 2016.

[18] *Vid.* Rodríguez Gómez, Nuria, "Teoría de la Oportunidad Diferencial de Richard A. Cloward y Lloyd E. Ohlin", *Revista Crimipedia*, 2015.

comportamiento de las personas que ponen de manifiesto su conducta conformista y no conformista en el espacio físico y el ciberespacio. Esta teoría integrada sostiene que las personas se comportan de manera diferente cuando se desplazan de un espacio a otro, basándose en que las personas que se reprimen de la conducta criminal en el espacio físico debido a su estatus y posición tienen una propensión a cometer delitos en el ciberespacio; que la identidad flexible, el anonimato disociativo, proveen a los ciberdelincuentes de los elementos para la elección de cometer cibercrímenes; y que la aventura intermitente de los agresores en el ciberespacio y la dinámica espacio-temporal natural del ciberespacio provee la oportunidad de escape para ellos.

De las teorías expuestas, la de las Actividades cotidianas/ rutinarias y la de las Oportunidades se consideran que son las más complejas, adecuadas y explicativas de la ciberdelincuencia por su capacidad de explicar de forma adecuada el fenómeno.

Frente a la primera visión que ofrecía la criminalidad informática de ser una modalidad de delincuencia muy específica, relacionada con concretas tecnologías y con reducidos usos de esta, hoy la única visión posible, por funcional, sobre la cibercriminalidad, es la de una delincuencia amplia, variada y cambiante que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social.[19] Entre sus características se destacan:

1. Anonimato: dado por el desconocimiento de la identidad del delincuente. La identidad real de este puede quedar oculta, o bien la conexión desde la cual realiza la acción delictiva. Tener conocimientos en la materia y habilidades necesarias permite a este sujeto, además de cometer el hecho, poder encubrirlo.

2. Inexistencia de barreras geográficas: Internet elimina la exigencia de proximidad entre agresor y víctima para la existencia de un delito. El ataque que se pude hacer desde cualquier parte del mundo, y pueden actuar sobre víctimas de otros lugares, reduciéndose las barreras que el espacio suele imponer para ello.

[19] Miró Llinares, Fernando, *El cibercrimen, fenomenología..., cit.,* p. 28.

3. Instantáneos: los ciberdelitos se cometen con gran celeridad e *ipso facto*. El perfeccionamiento del delito se da en el mismo momento en el que el delincuente lleva a cabo la acción. Se emplea poco tiempo en su comisión y el delito se consuma en cuestión de segundos.

4. Masivos: la masividad como característica de las TIC se ve reflejada en los ciberdelitos, dado que estas permiten la difusión masiva de contenidos. Además, la expansión del ámbito comunicativo al que puede acceder un agresor motivado, que supone el ciberespacio, conlleva una multiplicación de la potencialidad lesiva de una conducta por comparación con lo que ocurre en el espacio físico.

5. Pluriofensivos: pueden afectar a más de un bien jurídico protegido a la vez. Se vulnera el bien jurídico propiamente informático, a la vez que lesiona o pone en peligro otros bienes jurídicos tradicionales, como la intimidad, la indemnidad sexual, el honor, el patrimonio, la fe pública, el orden público.[20]

6. Son difíciles de demostrar, debido a los obstáculos que se presentan en la investigación de estos, por su carácter extremadamente técnico y sofisticado.

## 3. LA INFORMATIZACIÓN DE LA SOCIEDAD CUBANA, LA CIBERDELINCUENCIA Y SU TRATAMIENTO JURÍDICO PENAL

Cuba transita desde hace algunos años por un proceso que se ha definido como "informatización de la sociedad": uno de los tres pilares que respalda la gestión gubernamental. Las acciones realizadas, si bien aún no alcanzan la magnitud que demanda el desarrollo del país, han propiciado avances incuestionables en el gobierno y comercio electrónico.[21] La informatización de la sociedad cubana constituye el proceso de utilización ordenada y masiva de las Tecnologías de la Información y las Comunicaciones en la vida cotidiana para satisfacer las necesidades de todas las esferas de la sociedad, en su esfuerzo por lograr cada vez más eficacia y eficiencia en todos los procesos y por consiguiente mayor generación de riqueza y aumento en la calidad de vida de los ciudadanos.

---

[20] *Vid.* Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", *Revista chilena de Derecho*, Vol. 44, No. 1, Santiago de Chile, abril 2017.

[21] Puig Meneses, Yaima, "De la informatización de la sociedad a la transformación digital en Cuba", 13 de diciembre de 2021.

El desarrollo de las TIC es un tema que ha cobrado relevancia en Cuba como elemento determinante para el proceso de desarrollo actual de la sociedad. Existe la voluntad y disposición del Partido y el Gobierno cubano de desarrollar la informatización de la sociedad y poner Internet al servicio de todos y a lograr una inserción efectiva y auténtica de los cubanos en ese espacio.[22] Esta política del Estado cubano se ha materializado paulatinamente, y de ello es reflejo el avance y desarrollo de la conectividad en Cuba y la implementación y ampliación de los servicios de telefonía móvil e Internet.

Las TIC han alcanzado un desarrollo vertiginoso en Cuba en los últimos años, con gran aumento en la utilización de las redes sociales, trayendo consigo, además de sus nobles ventajas, números riesgos que ponen en peligro desde la seguridad de una nación hasta el patrimonio de sus ciudadanos. Conforme con el desarrollo experimentado con las TIC en los últimos años y la necesidad de enfrentar las conductas delictivas que se cometen en relación con esas tecnologías, tomando en cuenta además las disposiciones establecidas en los instrumentos internacionales, las experiencias del Derecho comparado y que la seguridad informática es hoy para cualquier país un problema de seguridad nacional, Cuba ha transitado con la reforma penal y procesal llevada a cabo, de un nulo reconocimiento de los ciberdelitos[23] a una regulación jurídica, en la Ley 151/2022, que introduce tipos delictivos específicos que tienen como bien jurídico protegido las tecnologías de la informática y las comunicaciones, agrupados bajo un título específico, Título IX, denominado "Delitos contra la integridad de las telecomunicaciones, las tecnologías de la información y la comunicación y sus servicios", y que reconoce como circunstancia de agravación de la sanción el uso inadecuado e ilícito de las tecnologías de la informática y las comunicaciones para la comisión de los delitos convencionales previstos en el Código.

---

[22] Así lo manifestó en el año 2015, el entonces primer vicepresidente de los Consejos de Estado y de Ministros, Miguel Díaz-Canel Bermúdez, en la clausura del Primer Taller Nacional de Informatización y Ciberseguridad, celebrado en La Habana, el 20 de febrero del 2015.

[23] NA: téngase en cuenta que el antiguo Código Penal, Ley 62 de 1987, data de una época en que el desarrollo informático en Cuba era incipiente, por lo que en él no se regulaban expresamente las diversas manifestaciones de ciberdelito; no obstante, ello no implicaba que esas manifestaciones delictivas quedaran impunes, pues la solución a ello era encuadrar esas conductas ciberdelictivas en otras modalidades que preveía el Código, ya sea mediante la forma de ejecución, el bien jurídico lesionado o el resultado.

El ordenamiento jurídico cubano ha dado sus primeros pasos desde la nueva Ley del Código Penal para enfrentar estos fenómenos, dejando relucir una voluntad política y legislativa de enfrentamiento contra el ciberdelito, que parte lógicamente de un reconocimiento de su existencia y de lo perjudicial que puede llegar a ser y ya está siendo.

Se ha incorporado como circunstancia agravante de la responsabilidad penal el hecho de facilitar la ejecución del hecho, imposibilitar u obstruir su descubrimiento, o agravar sus consecuencias, mediante la utilización de las tecnologías de la información y la comunicación, las telecomunicaciones y sus servicios. Es decir, que se considera circunstancia de agravamiento de la sanción el hecho de cometer el delito utilizando como medio, las tecnologías de la informática y las comunicaciones.

Se ha creado, y es lo más significativo, un título específico, Título IX, denominado "Delitos contra la integridad de las telecomunicaciones, las tecnologías de la información y la comunicación y sus servicios", en el que se establece un conjunto de conductas en donde el uso de las TIC es el medio empleado y el objetivo de ataque. En estos delitos el bien jurídico protegido por el tipo penal y vulnerado por el delito es la integridad de las comunicaciones, la informática y sus servicios.

## 4. LA CIBERDELINCUENCIA PATRIMONIAL. NOCIONES PARA SU DEFINICIÓN CONCEPTUAL

El término empleado en la investigación para identificar, dentro de la ciberdelincuencia como fenómeno social a aquella que afecta como bien jurídico los derechos patrimoniales, es el de "ciberdelincuencia patrimonial". Este término ha sido el asumido en esta investigación, pues en la doctrina no existe un término uniforme, algunos autores emplean el término "ciberdelincuencia económica",[24] otros el de "delitos informáticos de carácter patrimonial",[25] por lo que

[24] Esta terminología es empleada por autores como Miró Llinares. *Vid.* Miró Llinares, Fernando, *El cibercrimen, fenomenología..., cit*.

[25] Esta terminología es empleada por el autor, estudioso de la materia, Carlos María Romeo Casabona. Muestra de ello lo es su investigación denominada "Delitos Informáticos de carácter patrimonial", publicada en la *Revista Informática y Derecho* de la Universidad de La Laguna en el año 1996. *Vid.* Romeo Casabona, Carlos María, "Delitos Informáticos de carácter patrimonial", *Revista Informática y Derecho*, pp. 413-440.

en aras de ser consecuentes con la terminología empleada por la Ley sustantiva, Ley 151/2022, "Código Penal", vigente en Cuba,[26] se escogió el término ciberdelincuencia patrimonial.

Una de las expresiones más visibles de la ciberdelincuencia es la que se manifiesta para perjudicar la esfera patrimonial de terceros, que pueden ser personas naturales, personas jurídicas o el propio Estado. La ciberdelincuencia patrimonial es la utilización de la informática para la comisión de delitos patrimoniales; son todos aquellos delitos en los que la conducta típica de apropiación, defraudación o daño se lleva a efecto mediante la manipulación fraudulenta de documentos informatizados. Se trata de aquella actuación fraudulenta e ilícita, sobre medios informáticos, para obtener un beneficio provocando el perjuicio de un tercero.[27]

Haciendo un análisis dogmático de los tipos penales patrimoniales que recoge la Ley penal cubana, debe decirse que no todas las conductas en el título dedicado a proteger los derechos patrimoniales pueden ser cometidas mediante las TIC. Por lo que no todos los tipos penales encontrarán cabida en la ciberdelincuencia patrimonial, pues, por su propia naturaleza, no pueden ser llevados a cabo mediante el empleo de TIC.

## 5. TENDENCIAS DEL FENÓMENO DE LA CIBERDELINCUENCIA PATRIMONIAL QUE AFECTA A PERSONAS NATURALES EN CUBA

De las modalidades de ciberdelincuencia patrimonial en Cuba destaca, por ser la más usual, la estafa informática, ya sea mediante la suplantación de la identidad del usuario a partir de datos que este proporciona, o que se obtienen mediante el engaño para que comparta datos como el pin, el número de las

---

[26] NA: el título de los delitos que protegen los derechos patrimoniales en la Ley 151/2022, "Código Penal", es el Título XVII, el cual se denomina "Delitos contra los derechos patrimoniales". Bajo este título están recogidos los delitos de Hurto; Sustracción de electricidad, gas, agua o fuerza; Sustracción de vehículos de motor para usarlos; Robo con violencia o intimidación en las personas; Robo con fuerza en las cosas; Tenencia, fabricación y venta de instrumentos idóneos para ejecutar el delito de robo; Extorsión, Chantaje, Usurpación, Ocupación o disposición ilícita de locales o viviendas; Estafa; Apropiación Indebida; Receptación; Daños. *Vid.* Asamblea Nacional del Poder Popular, Ley 151/2022, "Código Penal".

[27] Corcoy Bidasolo, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Cuaderno del Instituto Vasco de Criminología*, No. 21, 2007, p. 16.

tarjetas magnéticas, la contraseña, los nombres y apellidos del dueño de la cuenta, el carnet de identidad, fotos, capturas de pantalla de las últimas operaciones registradas en Transfermóvil, o mediante el hackeo de las cuentas de los usuarios, utilizando la técnica del *phishing*. El fenómeno delictivo en cuestión tuvo su alza en 2021 como reflejo del cambio de la moneda y la informatización de la Sociedad.

Los modos de operar más usuales para consumar estas estafas son:

1. El SMS de confirmación de pago: Transfermóvil es la aplicación de pago más utilizada en Cuba para el comercio digital, y esta plataforma usa el envío de mensajes de texto (SMS) y códigos USSD para su funcionamiento, características de las cuales se aprovechan los ciberdelincuentes para engañar a sus víctimas. Una forma de estafa recurrente es el recibo de un SMS de confirmación de pago. Normalmente, cuando una persona realiza una transferencia puede agregar un número de teléfono al cual llega un SMS confirmando la transferencia. Esta forma de estafa está siendo muy utilizada, sobre todo utilizando como cebo el intercambio de divisas. Todo comienza con el anuncio tentador de compra o venta de divisas por las redes sociales Facebook, Telegram, WhatsApp, Revolico, un anuncio casi siempre desde un perfil falso. Cuando el usuario contacta el ciberdelincuente envía a este un SMS idéntico al que envía Transfermóvil como si hubiese realizado el pagado, y la víctima realiza la transferencia del efectivo para cerrar el negocio.

2. El Amigo falso de Facebook: otro engaño digital para estafar saldo móvil aprovecha las redes sociales para buscar posibles víctimas. El *hacker* se crea un perfil falso haciéndose pasar por un amigo de la persona objetivo y lo convence de que se le presentó un problema grande y necesita saldo móvil con urgencia, o alguna transferencia de efectivo.

3. SMS equivocado: es otro tipo de estafa para robar saldo móvil, se apoya en los mensajes de texto. El atacante envía un SMS haciéndose pasar por ETECSA. El mensaje recrea el texto que envía la empresa cubana cuando se realiza una transferencia de saldo. Acto seguido, el estafador envía otro SMS o la llamada en el que asegura que realizó una transferencia por una equivocación en el número de teléfono y pide de favor que le devuelvan su saldo.

4. Enlace engañoso: el ciberdelincuente envía un enlace al usuario con contenido tentador y cuando este abre el enlace para tener acceso al contenido, le

piden ingresar nuevamente los datos de nombre de usuario y contraseña. En el momento en el que estos datos son ingresados nuevamente, los *hackers* guardan esta información para entrar a las cuentas de los usuarios y buscar información útil además de embaucar a sus contactos con el mismo mensaje, con el objetivo de obtener un beneficio económico, empleando la técnica del *phishing*, pues buscan ganarse la confianza del usuario mediante el envío de un mensaje que enviaría alguien conocido. Ejemplo de esta forma de operar fue el famoso enlace denominado "¿Eres tú quien aparece en el video?".[28]

5. Los "cambietazos" de divisas, empleando como cebo a mujeres jóvenes sin antecedentes penales, de buena conducta. Son contratadas por vía digital por el autor de las defraudaciones, quien es desconocido para ellas, para que, en representación suya, participe en compra-venta de divisas con la persona que resulta ser afectada. En el contrato inicial que conciertan, vía digital, con el defraudador, estas jóvenes llenan una especie de formulario, donde facilitan sus datos de identidad, datos bancarios y contraseñas a solicitud del presunto empleador, quien les hace creer que se desempeñarán como gestoras de cobro en las operaciones de compra y venta de moneda dura. Al momento de la transacción, el tercero con el que acuerda el defraudador, previamente y vía *on line*, la operación de cambio, transfiere el dinero en presencia de estas jóvenes, y una vez las jóvenes informan del éxito de la transferencia al defraudador, estas resultan bloqueadas de acceder a su cuenta, y el defraudador se apropia del dinero que estas poseían y del dinero transferido por las víctimas.

6. Seguidamente, como modalidad más recurrente, el Robo con fuerza en las cosas mediante el empleo de herramientas digitales que burlan barreras de seguridad, las cuales el ciberdelincuente adquiere de grupos clandestinos especializados en temas de hackeo, que existen en las redes sociales Telegram y WhatsApp. En el caso de WhatsApp, el grupo se denomina "Anonymus", y está dirigido, fundamentalmente, a la creación de programas informáticos capaces de sustraer informaciones bancarias, tanto en sitios de comercio electrónico como en pasarelas de pago. En el caso de Telegram, el grupo se denomina "The Death Zone" y está diseñado para el escaneo y explotación de vulnerabilidades en plataformas web. Siendo así, con el fin de descubrir fisuras de la seguridad en las plataformas de

[28] *Vid*. *Cubadebate*, "¿Eres tú en el video? No abras el link de Messenger", 5 de abril de 2022.

instituciones estatales, económicas y militares cubanas y obtener información sobre su funcionamiento y los usuarios que la emplean, los ciberdelincuentes utilizan esas aplicaciones digitales, obteniendo los datos sin autorización de los usuarios legítimos, luego acceden a las cuentas con esa información, cambian los accesos y las contraseñas, y transfieren, escalonadamente, la cuantía deseada a cuentas bancarias que utilizan como puentes.

## 6. ANÁLISIS CRIMINOLÓGICO DE LA CIBERDELINCUENCIA PATRIMONIAL QUE AFECTA A PERSONAS NATURALES EN CUBA

Para llevar a cabo el análisis criminológico de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba se tomaron como referencia los casos de ciberdelincuencia patrimonial aportados por la Fiscalía General de la República, el Departamento de Control al Órgano Especializado de Investigación Criminal de los Delitos Comunes de la Fiscalía Provincial de La Habana y las Unidades Territoriales de Investigación Criminal No. I y No. III; además, se tomaron en cuenta las respuestas de las encuestas aplicadas a usuarios de las redes y los resultados de las entrevistas realizadas a especialistas en la materia. Para exponer el resultado obtenido se tuvieron como parámetros los siguientes elementos: características del imputado, características de las víctimas, las oportunidades delictivas que propiciaron el hecho y los obstáculos enfrentados durante la fase investigativa del delito.

**a) En cuanto a las características de los ciberdelincuentes:**

En los procesos donde la investigación permitió llegar al ciberdelincuente se evidenció que en el actuar de estos expusieron motivaciones económicas, sociales o personales. En los casos estudiados, los comisores de los hechos actuaban con evidente ánimo de lucro, pero también asumían sus hechos como un evidente reto personal de superación. En la mayoría de los casos, los ciberdelincuentes eran hombres jóvenes, con edades de entre 18 y 35 años de edad, con una formación empírica en la informática, pero muy hábiles, con interés y curiosidad en la informática, las redes y el mundo virtual.

La casi totalidad de ellos carecía de antecedentes penales, y se trataba de individuos desocupados laboralmente. Estos imputados confesaron su participación y contribuyeron al esclarecimiento de los hechos. Se trata de personas que aprenden a navegar por la red y a delinquir a través de páginas webs, blogs o

foros, por lo que, aunque en la mayoría de los casos son personas con conocimientos, no suelen haber recibido formación profesional. Tampoco existe una relación entre el nivel educacional o cultural y el perfil de los ciberdelincuentes. Se trata de personas dispuestas a aprender, con elevada autoestima y seguras de sí mismas.

Durante el estudio de los casos, se advirtió que estos muchachos comenzaron su actividad motivados por la curiosidad, por lo que tanteaban por los sistemas informáticos, luego de detectar las vulnerabilidades de estos, o llevando al error a los usuarios de las redes, lo cual refuerza la idea de que el ciberdelincuente se aprovecha de las brechas de seguridad en los sistemas informáticos y de la colaboración involuntaria de sus víctimas.

**b) Características de las víctimas:**

Para hacer referencia a este punto del estudio, es necesario aclarar que la mayoría de las personas que han resultado víctimas, específicamente de las estafas informáticas, son personas no nativas digitales, con acceso a Internet, cuentas bancarias activas, que usualmente operan con las plataformas de pago, y que realizan un uso inadecuado de los sistemas informáticos, actúan con ingenuidad y desconocimiento de los riesgos; ejemplo de ello es la poca protección de sus activos, por ejemplo, contraseñas muy fáciles de memorizar. Por otro lado, cuando se trata de los robos con fuerza en las cosas cometidos luego de forzar sistemas informáticos, se aprecia que la víctima puede ser cualquier usuario de la red, de cualquier edad. Aquí las víctimas no participan en la cadena causal que da al traste con la sustracción del patrimonio, ellas no contribuyen con su actuar al resultado delictivo.

**c) Oportunidades delictivas:**

Las características del ciberespacio constituyen una de las oportunidades delictivas que propician los hechos de ciberdelincuencia; entre ellas: el alcance del ciberespacio, debido a la ausencia de fronteras, posibilita que una acción iniciada en un punto termine afectando de forma casi instantánea a elementos situados en cualquier parte del mundo; la asimetría de este espacio, dado que el acceso al ciberespacio es global, sencillo y económico, tal es así que un individuo o pequeña organización pueden, con un mínimo de capacidad técnica y recursos, producir efectos en un oponente con el que se guarda total desproporción; y el anonimato, pues la utilización de identidades virtuales facilita la ocultación de la verdadera personalidad e intenciones de individuos o grupos.

Es fenómeno frecuente usurpar la identidad de terceros para ocultar las actividades propias, lo cual tributa a que la atribución de estas actividades se convierte en un problema fundamental, siendo necesario combinar múltiples disciplinas del área de la inteligencia y del análisis forense para lograr resultados.

Las redes sociales son de libre acceso a nivel internacional, por lo que el ciberdelincuente se vale de la posibilidad de ocultar su identidad real, o asumir una identidad falsa, ya sea suplantando identidades existentes de terceros ajenos al acto, o creando perfiles falsos.

El grado de sofisticación del ejecutante incrementa la dificultad de la atribución de responsabilidad e incluso puede hacerla imposible. Esto a su vez constituye una de las oportunidades delictivas, pues dificulta el control social formal de este tipo de delitos y con ello se favorece la impunidad de estas conductas, lo cual es una circunstancia que motiva al ciberdelincuente a operar sin el riesgo de ser capturado.

La ingenuidad, el exceso de confianza y el desconocimiento demuestran la baja percepción del peligro en los usuarios de las redes y víctimas de estos delitos, constituyendo esta la primera oportunidad delictiva que favorece las manifestaciones de ciberdelincuencia patrimonial en Cuba.

Las brechas de seguridad en los sistemas bancarios nacionales y en los sistemas de ciberseguridad de instituciones, organizaciones y entidades estatales y no estatales constituyen una vulnerabilidad peligrosa que deviene oportunidad delictiva.

**d) Obstáculos investigativos enfrentados:**

Resulta muy difícil la investigación de sus actos y su demostración, dado el carácter técnico y sofisticado de este tipo de delitos. Para el esclarecimiento del hecho es de vital relevancia la información aportada por los propios imputados, quienes dan información respecto a la dinámica del hecho; elementos sin los cuales sería muy difícil reconstruir el hecho para describir la conducta por él realizada para producir el resultado delictivo.

Como vulnerabilidades en las investigaciones se aprecia que existe falta de conocimientos informáticos, falta de preparación en la investigación de estos delitos, falta de herramientas investigativas específicas para esta tipología

delictiva, así como se carece de una metodología que indique cómo ordenar lógica y metodológicamente la investigación en aras de optimizar los recursos y no perder tiempo. Ello indica fallas en el control social formal, que vienen dadas especialmente por la falta de un sistema de enfrentamiento adecuado y preparado para combatir estas conductas delictivas.

Generalmente, no son denunciados por diversos motivos, como la indiferencia y el desconocimiento, o el temor a ser procesados por los delitos en los cuales incurrían, dígase tráfico ilegal de divisas, quedando la mayoría de estas conductas impunes. Por otro lado, el número de víctimas es mucho mayor que las cifras de personas que efectivamente denuncian. En particular, este tipo de modalidad delictiva que es la estafa informática, cuando esta tiene lugar con el móvil de compra y venta de divisas, tiene como peculiaridad que las personas se abstienen de denunciar por el temor a ponerse en evidencia como autores del delito de tráfico ilegal de divisas o monedas. Por otro lado, muchas de las denuncias son realizadas de oficio por funcionarios del banco, luego de que los clientes acuden a la sucursal bancaria donde se obtuvo el soporte electrónico y reportaran la defraudación en su patrimonio; así mismo sucede con la Empresa de Telecomunicaciones de Cuba, cuando la defraudación es mediante el robo de saldo en los servicios telefónicos móviles.

## 7. PROPUESTAS PARA DISMINUIR LOS RIESGOS DE OCURRENCIA DE LA CIBERDELINCUENCIA PATRIMONIAL A PARTIR DEL ANÁLISIS DE SUS OPORTUNIDADES DELICTIVAS

En el caso de la ciberdelincuencia patrimonial, además de los costos económicos, existen impactos menos tangibles, incluyendo la pérdida de confianza en el comercio electrónico, la erosión de la privacidad individual y la disminución de la confianza en los servicios en línea. Ello, unido a la gravedad de no accionar frente a un fenómeno en auge, que muestra señales de su significación social, incluso al nivel de constituir un problema de seguridad nacional, hace que sea imprescindible diseñar estrategias de prevención de este fenómeno.

Es reconocido, y así lo demostró el estudio de los casos de Estafa Informática analizados, que las personas son el eslabón más débil de la cadena de la seguridad. Ello implica que, aunque tradicionalmente el abordaje analítico de la problemática ha estado dirigido al diseño de soluciones orientadas fundamentalmente hacia las infraestructuras de comunicación, los dispositivos y las aplicaciones, se ha olvidado que el factor humano es un elemento activo

para garantizar la seguridad. Es por ello que debe trabajarse en función de que las personas usuarias de las reden dejen de ser sujetos pasivos que necesitan ser protegidas para convertirse en agentes activos, en guardianes de su seguridad, y la seguridad de su información, datos y sistemas informáticos.

Es necesario trabajar en la prevención general y en la educación ciudadana frente al fenómeno. Ello deberá partir de la exposición del alcance e incidencia de esta tipología delictiva en Cuba; debe crearse una cultura de cómo evitar ser víctima de estos delitos, cómo proteger los datos personales y qué hacer en caso de ser víctima de estos. El punto de partida debe ser el entendido de que la baja percepción del riesgo en la población usuaria de las redes, la ingenuidad y el desconocimiento constituyen una de las principales oportunidades delictivas que propician este tipo de manifestaciones, lo que demuestra que es imperioso elevar la percepción de riesgo respecto a estos ilícitos en la población, mediante estrategias de comunicación y educación.

En este sentido, es recomendable instruir a los usuarios de las redes en que deben abstenerse de aportar datos personales a desconocidos o colocarlos en plataformas de redes sociales, pues estas luego son utilizadas por los ciberdelincuentes como fuente de información y selección de las víctimas; deben chequear sistemáticamente las cuentas personales; deben utilizar el doble factor de autenticación, que es una medida de seguridad que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta, que requiere, además de la contraseña habitual, un código de seguridad adicional; deben emplear contraseñas fuertes, que son aquellas contraseñas seguras en las que combinan números, letras y símbolos, incluyen de 16 a 20 caracteres y no se comparten con nadie; deben atender las alertas, vía correo electrónico, sobre intentos de acceder a sus cuentas por dispositivos distintos a los usualmente utilizados, elementos que deben tenerse en cuenta, porque constituyen mecanismos de seguridad que blindan las cuentas e impiden el acceso de terceras personas; no deben hacer clic en enlaces sospechosos y deben ser cautelosos con los correos electrónicos y mensajes inesperados; no deben guardarse las claves o contraseñas junto con sus tarjetas; no deben hacer pública información impresa en las tarjetas; no deben informar a desconocidos datos del carné de identidad, número, tomo o folio.

Así mismo, el Banco Central de Cuba recomienda que no se debe facilitar o entregar los números de las tarjetas magnéticas, contraseñas, ni el PIN, tampoco los nombres y apellidos del dueño de la cuenta, carnet de identidad, fotos, ni capturas de pantalla de las últimas operaciones registradas en Transfermóvil,

pues toda esta información suele pedirla el estafador para suplantar la identidad en EnZona, logrando así el acceso a los fondos de sus víctimas.

Por otro lado, la Empresa de Telecomunicaciones implementó desde el año 2017 una campaña denominada "¡Navegue seguro!", en la cual se ofrece una serie de recomendaciones a sus clientes, como verificar que la dirección web del portal de autentificación comience con *https* y que al pinchar en el candado de arriba, a la izquierda, se muestre el certifico de seguridad.

En otro sentido, es necesario recalcar que la rápida evolución de las TIC ha propiciado que la ciberseguridad resulte una condición fundamental para garantizar el desarrollo seguro de actividades básicas en la sociedad moderna. Es por ello que es esencial trabajar y reforzar la ciberseguridad de las plataformas y sistemas digitales en Cuba, pues constituyen las brechas de seguridad una de las oportunidades delictivas que, actualmente, propician las manifestaciones ciberdelictivas. Debe diseñarse un correcto sistema de ciberseguridad en las entidades estatales y no estatales, y reforzar aquellas que aún presentan vulnerabilidades. Ello debe partir de reconocer que proteger la información y los sistemas informáticos ante las amenazas de las que son vulnerables, es una tarea de suma importancia, que se vincula con la seguridad de la información que se maneje y circule por las redes de entidades, las cuales pueden alcanzar a los usuarios, los clientes y la nación.

La seguridad de la información se consigue con actuaciones que garanticen tres propiedades: confidencialidad, integridad y disponibilidad. Es la información el bien más preciado a proteger y preservar. Es por ello que se deben seleccionar e implementar controles o contramedidas que ayuden a reducir el riesgo que representan las vulnerabilidades.

La ciberseguridad constituye la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las instituciones tienen la responsabilidad de proteger los datos, dispositivos, servidores y las redes frente a posibles amenazas. Para ello deben utilizar medidas y herramientas de ciberseguridad que garanticen la protección de los datos confidenciales del acceso no autorizado e interrupciones en las operaciones debido a una actividad de red no deseada. El éxito de un ciberataque produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Para la implementación de estrategias de ciberseguridad debe contarse con especialistas de ciberseguridad, que evalúen los riesgos de seguridad de los sistemas informáticos existentes, redes, almacenamiento de datos, aplicaciones y

otros dispositivos conectados, y que, a partir de los análisis, creen un marco de ciberseguridad integral e implementan medidas protectoras en la entidad.

Es por ello que se requiere de un equipo de especialistas, capacitados, que cuenten con las herramientas técnicas, tecnológicas, para desarrollar un adecuado sistema de ciberseguridad, en el que se empleen tecnologías de defensa cibernética constituido por varias capas de protección contra posibles amenazas en todos los puntos de acceso a datos, capaces de identificar el riesgo, proteger identidades, infraestructura y los datos, detectar anomalías, responder y analizar la causa raíz y realizar la recuperación después de un evento de ciberataque. Por otro lado, la formación y educación de los empleados con respecto a los principios de ciberseguridad reduce los riesgos de descuidos que pueden dar lugar a incidencias no deseadas.

Una cuestión a tener en cuenta son los aspectos relacionados con el control social formal e informal, los cuales están muy a tono con la pretensión de sentar los fundamentos criminológicos para entender el fenómeno de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba. En este sentido, publicitar el trabajo que realiza el país en aras de desarrollar estrategias de ciberseguridad, exponer los casos de ciberdelincuencia que se den en el país, cómo se investigan y esclarecen estos hechos, así como mostrar las consecuencias jurídico-penales de los responsables puede servir de freno inhibitorio a los ciberdelincuentes, máxime cuando se ha advertido que una de las oportunidades delictivas en este tipo de conductas es la confianza en la impunidad de sus conductas.

En este orden de ideas, implementar una correcta estrategia comunicativa en la que se instruya a la población en la ciberseguridad, en cómo protegerse de ciberataques y en cómo reaccionar ante estas conductas, sobre la base de lo perjudicial que pueden llegar a ser, contribuirá a fomentar en estas personas una cultura de repudio a estas conductas lesivas, lo cual influirá en la labor de rechazo y enfrentamiento a estas conductas.

## 8. A MODO DE CONCLUSIONES

Los fundamentos criminológicos que permiten el abordaje de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba parten de reconocer al ciberespacio como un nuevo espacio criminógeno, como resultado de las características que *per se* posee, caracterizado por pocos riesgos para el ciberdelincuente y abundantes objetivos vulnerables. Por otro lado, se encuentran

las oportunidades criminales que son aprovechadas por el ciberdelincuente, como son sus conocimientos informáticos, el desconocimiento, la ingenuidad y la baja percepción del peligro en los usuarios de las redes, las vulnerabilidades, brechas de seguridad de los sistemas informáticos y las fallas en el control social formal de esta nueva forma de delincuencia, dadas por las deficiencias investigativas, la impunidad de la cual gozan y la falta de cultura en denunciar estas conductas, manifestados en las altas cifras negras de criminalidad.

La prevención de esta modalidad delictiva, en lugar de concentrar exclusivamente la atención en el ciberdelincuente, debe prestar más atención al propio acto delictivo y a los factores situacionales. Es por ello que las estrategias preventivas deben ser diseñadas desde un enfoque situacional, dirigido a neutralizar las oportunidades que facilitan su comisión, para, de esta forma, disminuir las posibilidades de realización del delito, por lo que se necesita trabajar en la educación de la población, reforzar los mecanismos de ciberseguridad en la nación y fortalecer el sistema de enfrentamiento, lo que incrementará la percepción del riesgo por el comisor de estos hechos y servirá de freno inhibitorio de estas conductas delictivas.

El estudio pretendió ser un acercamiento criminológico al fenómeno en Cuba, con vistas a desarrollar estrategias preventivas, toda vez que se trata de un fenómeno que va adquiriendo interés por el incremento experimentado y sus consecuencias, en una nación que se abre digitalmente. La solución no será jamás frenar el desarrollo tecnológico, sino direccionarlo de una forma segura, previniendo y enfrentando todo ataque o riesgo en este empeño. Algo que, necesariamente, deberá partir del diseño de un sistema de ciberseguridad robustecido y del desarrollo de una cultura, educación y concientización digital de la población.

## REFERENCIAS BIBLIOGRÁFICAS

### FUENTES DOCTRINALES:

Acosta, María Gabriela; Milko Benavides Merck y Nelson Patricio García, "Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios", *Revista Venezolana de Gerencia*, Vol. 25, No. 89, 2020.

Aguilar Cárceles, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", *Revista Criminalidad,* Vol. 57, No. 15, 2015, disponible en https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/165

Agustina Sanllehí, José, "La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual", *Revista International e-Journal of Criminal Sciences*, Artículo 4, No. 3, 2009.

Anguita Osuna, José Enrique, "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea", *Revista de Estudios en Seguridad Internacional*, Vol. 4, No. 1, 2018, pp. 107-126, disponible en http://dx.doi.org/10.18847/1.7.7

Atiénzar Rivero, Enrique, "Estafas entre redes", *Cubadebate*, 16 de abril del 2023, disponible en http://www.cubadebate.cu/especiales/2023/04/16/estafas-entre-redes/

Benito, María, "Ciberdelincuencia: ¿qué es y cómo combatirla?", *Blog de los Estudios de Derecho y Ciencia Política, IurisCrimPol,* 15 de junio del 2023, disponible en https://blogs.uoc.edu/edcp/es/ciberdelincuencia-que-es-y-como-combatirla/

Blog de Actualidad de la transformación digital, disponible en https://ginzo.tech/doble-factor-autenticacion/

Borrego, Mary Luz, "Estafas virtuales: en la confianza está el peligro", periódico *Escambray,* 10 de marzo del 2022, disponible en https://www.escambray.cu/2022/estafas-virtuales-en-la-confianza-esta-el-peligro/

Bueno De Mata, Federico*, Prueba electrónica y proceso 2.0*, tirant lo blanch, Valencia, 2014.

Cabrera Cabrera, Xiomara, "La prevención victimológica en Cuba. Insuficiente protección del Derecho Penal", *Revista Contribuciones a las Ciencias Sociales*, marzo 2012, disponible en https://ideas.repec.org/a/erv/coccss/y2012i2012-0318.html

Cabrera Quiroz, Marycarmen, "Fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el período 2010-2018", *Repositorio de la Universidad Privada del Norte*, disponible en https://hdl.handle.net/11537/24533

Cámara Arroyo, Sergio, "Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente", *Revista Derecho y Cambio Social*, No. 60, abril-junio 2020.

Campoy Torrente, Pedro y Lucia Summers, "Los precipitadores situacionales del delito: otra mirada a la interacción persona-ambiente", *Revista Criminalidad*, Vol. 57, No. 3, 2015.

Castells, Manuel, *La era de la información. Fin de milenio*, Alianza editorial, Madrid, 1998.

Castro Espina, Sandra Jeannette, *Algunos aspectos dogmáticos de la delincuencia informática*, 2007, disponible en https://dialnet.unirioja.es/descarga/articulo/3313831.pdf

Catá del Palacio, Arturo, *Ciberdelincuencia. Desarrollo y persecución tecnológica,* Universidad Politécnica de Madrid, 2014, disponible en https://oa.upm.es/34795/

"Ciberdelincuencia: tipos y medidas de prevención", 17 de enero 2022, disponible en https://www.redseguridad.com/actualidad/cibercrimen/que-es-la-ciberdelincuencia-y-como-se-puede-prevenir_20220117.html

Corcoy Bidasolo, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", *Cuaderno del Instituto Vasco de Criminología*, No. 21, 2007.

Cordero Ruiz, Nuria Fernanda, "La ciberdelincuencia", *Máster Universitario en Acceso a la Profesión de Abogado*, Universidad de Alcalá, 2021, disponible en https://ebuah.uah.es/dspace/handle/10017/49563

*Cubadebate,* "¿Eres tú en el video? No abras el link de Messenger", 5 de abril del 2022, disponible en http://www.cubadebate.cu/noticias/2022/04/05/eres-tu-en-el-video-no-abras-el-link-de-messenger/

De Armas Fonticoba, Tania y Ángela Gómez Pérez, *Introducción a la Criminología,* Félix Varela, La Habana, 2015.

De la Cuesta Arzamendi, Jorge Luis y Ana Isabel Pérez Machío, "Ciberdelincuentes y Cibervíctimas", en *Derecho penal informático*, Civitas y Thomson Reuters, Pamplona, disponible en https://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf

De Pedro Baena, Nerea, "¿Cómo es el perfil del ciberdelincuente?", Boletín semanal *Lisa News*, 2022, disponible en https://www.lisanews.org/ciberseguridad/como-es-el-perfil-del-ciberdelincuente/

Del Sol González, Yaditza, "Wifi falsa y otros delitos en la red cubana", *Granma*, La Habana, 12 de junio de 2024.

*Juventud Rebelde, Diario de la Juventud cubana,* 17/6/2022, disponible en https://www.juventudrebelde.cu/cuba/2022-06-22/mas-de-7-5-millones-de-cubanos-con-internet

Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución. El Convenio de Budapest", *Revista Electrónica de Derecho de La Universidad de la Rioja (REDUR)*, No. 8, 2010, pp. 169-203, disponible en https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

Díaz Hernández, Rosa M. y Zulariam Pérez Martí, "Estafa en la WiFi: Robo de cuentas y otros ciberdelitos en Cuba", *Cubadebate*, 17 de diciembre de 2017, disponible en http://www.cubadebate.cu/especiales/2017/12/17/estafa-en-la-wifi-robo-de-cuentas-nauta-y-otros-ciberdelitos-en-cuba/

División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias. Sector de Desarrollo de las Telecomunicaciones de la UIT, "El ciberdelito: Guía para los países en desarrollo", Proyecto de abril de 2009, disponible en https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

Espinosa Bejerano, Santiago, "La ciberseguridad, el ciberespacio, internet y las tecnologías de la información y las comunicaciones", disponible en http://www.cubadebate.cu/especiales/2021/09/04/la-ciberseguridad-el-ciberespacio-internet-y-las-tecnologias-de-la-informacion-y-las-comunicaciones/

Evaristo Abril, Domingo; Miguel López-Coronado; Rafael Mompó Gómez, "La necesidad de indicadores sociales y económicos para el estudio de la evolución de la sociedad de la información", *Revista de investigación económica y social de Castilla y León*, No. 1, 1999, pp. 73-86.

Fernández Romo, Rodolfo y Waldemar Paulo Da Silva José, "Aristas criminológicas de la delincuencia informática", *Serie Ciencias Penales y Criminológicas. Interrogantes, alternativas y desafíos en clave de Derecho Penal y Criminología*, disponible en https://cuba.vlex.com/vid/aristas-criminologicas-delincuencia-informatica-690582601

García García, Diego Eloy, "El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016)", *Revista Boliviana de Derecho*, No. 25, Santa Cruz de la Sierra, 2018, disponible en http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025

García García, Gelsy, "Acceso y uso de las Tecnologías de la Información y Comunicación en la Cuba actual", *Revista de Estudios del Desarrollo Social: Cuba y América Latina*, Vol. 3, No. 2, mayo-agosto 2015, pp. 1-53, disponible en https://www.redalyc.org/pdf/5523/552357189011.pdf

García García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", *Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, No. 74, mayo-agosto 2008, disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=289096

GIL, Leandro (coord.), *Cibercrimen y delitos informáticos. Guía de Estudio,* año 2021, disponible en https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

Goite Pierre, Mayda, "Delitos contra los derechos patrimoniales", en Colectivo de Autores, *Derecho Penal Especial,* Tomo II, Félix Varela, La Habana, 2005.

Goite Pierre, Mayda; Rodolfo Fernández Romo, Francisco Marcelo Obando Freire, Andrés Obando Ochoa y Santiago Velásquez Velásquez, "La prevención situacional del delito", Serie *Ciencias Penales y Criminológ*icas. "El Derecho Penal y la Criminología. Su Práctica en Angola, Cuba y Ecuador en el siglo XXI", julio 2019, disponible en https://cuba.vlex.com/vid/prevencion-situacional-delito-844293915

Gómez Pérez, Ángela, "Aspectos puntuales acerca de la Victimología", Tema VII, en Colectivo de Autores, *Manual de Criminología*, Félix Varela, La Habana, 2004.

González Fuentes, Yisel, "¿Cómo evitar las estafas mediante tarjetas magnéticas?", *Granma*, 13 de agosto de 2021, disponible en https://www.granma.cu/cuba/2021-08-13/como-evitar-las-estafas-mediante-tarjetas-magneticas-10-08-2021-20-08-11

González Rus, Juan José, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", *Revista de la Facultad de Derecho de la Universidad Complutense,* No. Extra 12, 1986.

Gorostidi, Jon López, "Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia", *Revista chilena de Derecho y Tecnología*, Vol. 11, No. 1, Santiago de Chile, junio 2022, disponible en https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100121&lng=es&nrm=iso

Gutiérrez Francés, María Luz, "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual", *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja (REDUR*), No. 3, 2005.

Hernández Díaz, Leyre, "El delito informático", *Revista Eguzkilore: Cuaderno del Instituto Vasco de Criminología,* No. 23, San Sebastián, diciembre 2009, disponible en https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Herrera Gandol, Dimas Alfredo, "Conductas definidas como delitos informáticos o ciberdelitos en la legislación nacional y el derecho comparado", 2020, disponible en https://www.fgr.gob.cu/en/node/6954

Hikal, Wael, "Los factores criminógenos exógenos", *Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la Universidad de Valencia*, 2009, disponible en https://www.uv.es/iccp/recrim/recrim09/recrim09n07.pdf

Hikal-Carreón, Wael Sarwat, "La especialización de la criminología: De lo general a lo específico, ¿hacia una neocriminología? Teoría de las criminologías específicas", *Revista Derecho y Cambio Social*, Vol. 10, No. 32, 2013.

Jaishankar, Karuppannan, "Cyber criminology: Evolving a novel discipline with a new journal International", *Journal of Cyber Criminology*, 2007.

Jamidulin, Airat, "Ciberdelincuencia: un instrumento de injerencia en los asuntos internos de los Estados", *Juventud Rebelde*, 11 de julio del 2019, disponible en https://www.juventudrebelde.cu/ciencia-tecnica/2019-07-10/ciberdelincuencia-un-instrumento-de-injerencia-en-los-asuntos-internos-de-los-estados

Jiménez Rozas, Jéssica, "CIBERDELINCUENCIA: evolución y relación con la actual situación de pandemia. Nuevas modalidades y nuevas problemáticas", *Trabajo fin de grado curso de adaptación al grado en Criminología*, junio de 2022, disponible en https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y

Kigerl, Alex, "Interrumpir el proceso de aparición de la ciberdelincuencia: de los delincuentes motivados a los ciberataques", *6to Informe Internacional Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia*, Montreal, 2018, disponible en: https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

Koops, Bert-Jaap, "The internet and its opportunities for cybercrime, Transnational Criminology", *Manual I,* 2010.

Lamperti, Sabrina, "Problemáticas en torno a la investigación de los delitos informáticos", Universidad Fasta Federación Iberoamericana de Asociaciones de Derecho e Informática. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática, Mar del Plata, 2014, disponible en https://www.researchgate.net/publication/324064192_Problematicas_en_torno_a_la_Investigacion_de_delitos_informaticos

Littlejohn Shinder, Debra, *Prevención y detección de delitos informáticos*, Anaya, Madrid, 2003.

Llano Pereira, Irma, *El desafío de la cooperación internacional, el cibercrimen y la justicia penal en el ciberespacio*, Seminario de la Unión Europea y del Consejo de Europa con las regiones de América Latina y el Caribe, Paraguay, 2020, disponible en https://rm.coe.int/cibercrimen-y-la-justicia-penal-en-el-ciberespacio-irma/16809f0321

Mata y Martín, Ricardo Manuel, "Criminalidad informática: una introducción al cibercrimen", *Revista Actualidad Penal*, No. 36, 2003.

Mata y Martín, Ricardo, *Delincuencia informática y Derecho Penal*, Hispamer, Nicaragua, 2003.

Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", *Revista chilena de Derecho,* Vol. 44, No. 1 2018, disponible en https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011

Medina Gómez, Diana, "Los delitos cibernéticos y los problemas a enfrentar", *Revista jurídica de la UNAM*, 2020, disponible en https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543

Miró Llinares, Fernando, "Crimen, cibercrimen y COVID-19. Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", *Revista de Internet, derecho y política,* No. 32 2021, disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=7962061

Miró Llinares, Fernando, "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", *Revista Electrónica de Ciencia Penal y Criminología*, No. 13, 2011, disponible en https://dialnet.unirioja.es/servlet/articulo?codigo=4396388 [consultado el 11/4/2023, a las 20.00].

Miró Llinares, Fernando, *Delincuencia asociada al uso de las TIC*, Universitat Oberta de Catalunya, disponible en http://cv.uoc.edu/annotation/49e137c73e26ddcd8cd71e5e8e4b66cd/803643/PID_00195946/PID_00195946.html

Miró Llinares, Fernando, *El cibercrimen, fenomenología y criminología de la delincuencia en el ciberespacio,* Ediciones Jurídicas y Sociales. S.A., Marcial Pons, Madrid, 2012.

Mora, Endira; Yoselin Sánchez, Oscar González y Daniel Quintero, "Los delitos informáticos: experiencia investigativa en CENDITEL", *Revista Conocimiento Libre y Licenciamiento,* No. 16, 2017, disponible en https://convite.cenditel.gob.ve/revistaclic/index.php/revistaclic/article/view/908

Morales Delgado, Deivid Yuly, "La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Universidad Señor de Sipán", Perú, 2015, disponible en https://repositorio.uss.edu.pe/handle/20.500.12802/3161

Ortiz Pradillo, Juan Carlos, "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica", en Julio Pérez Gil (coord.), *El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito*, La Ley, Madrid, 2012.

Ortiz Pradillo, Juan Carlos*, La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, Fundación Alternativas, Madrid, 2013.

Patiño Ortega, María, "Teoría de la elección racional de Cornish y Clarke", *Crimipedia*, revista editada en Elche por el Centro Crímina para el Estudio y Prevención de la Delincuencia, 2016, disponible en https://crimipedia.umh.es/topics/teoria-de-la-eleccion-racional-de-cornish-y-clarke/

*Granma*, "Wifi falsas y robo de cuentas Nauta en zonas públicas de acceso a internet en Cuba", 27 de diciembre del 2017, disponible en https://www.escambray.cu/2017/wifi-falsas-y-robo-de-cuentas-nauta-en-zonas-publicas-de-acceso-a-internet-en-cuba/

Puig Meneses, Yaima, "De la informatización de la sociedad a la transformación digital en Cuba", 13 de diciembre de 2021, disponible en https://www.presidencia.gob.cu/es/noticias/de-la-informatizacion-de-la-sociedad-a-la-transformacion-digital-en-cuba/

Restrepo, Hugo Armando, "Comercio electrónico: Importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra online y en redes sociales en Colombia", Trabajo de grado presentado como requisito para optar al título de Ingeniero de sistemas. Universidad Nacional Abierta y a Distancia UNAD, marzo 2023.

Rincón Ríos, Jarvey, "El delito en la cibersociedad y la justicia penal internacional", *Tesis Doctoral para optar al grado de Doctor*, Madrid, 2015, disponible en https://eprints.ucm.es/33360/

Rodríguez Gómez, Nuria, "Teoría de la Oportunidad Diferencial de Richard A. Cloward y Lloyd E. Ohlin", *Crimipedia,* revista editada en Elche por el Centro Crímina para el Estudio y Prevención de la Delincuencia, Alicante, España, 2015.

Rojo Ramos, Jorge; Carlos Ferrera-Granados, Carlos Mañanas Iglesias y Juan Carlos Guevara Pérez, "Estudio descriptivo de Cibervictimización en una muestra de estudiantes de Educación Secundaria Obligatoria", *Revista Electrónica Interuniversitaria de Formación del Profesorado,* Vol. 25, No. 1, 2022, disponible en https://dialnet.unirioja.es/descarga/articulo/8272669.pdf

Romeo Casabona, Carlos María e Iñigo de Miguel Beriain, *El cibercrimen económico y patrimonial. Guía Docente,* Departamento de Derecho Público y Cátedra Interuniversitaria, Diputación Foral de Bizkaia, de Derecho y Genoma Humano, Universidad del País Vasco, disponible en https://ocw.ehu.eus/mod/resource/view.php?id=32682

Romeo Casabona, Carlos María y Miguel Beriain, *El cibercrimen en el ámbito económico y patrimonial,* Universidad del País Vasco, Euskal Herriko Unibersitatea, disponible en https://ocw.ehu.eus/mod/resource/view.php?id=32683

Romeo Casabona, Carlos María, "Delitos Informáticos de carácter patrimonial", revista *Informática y Derecho,* Universidad de La Laguna, 1996, disponible en https://dialnet.unirioja.es/descarga/articulo/248763.pdf

Salomón Clotet, Juan, "Delito informático y su investigación. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?", *Cuadernos de derecho judicial,* No. 3, 2006.

Sánchez Vera, Fulgencio; Javier Eloy Martínez Guirao y Anastasia Téllez Infantes, "La seguridad en el ciberespacio desde una perspectiva sociocultural", *Methaodos, Revista de Ciencias Sociales,* 2022, Vol. 10, No. 2, p. 244, disponible en https://doi.org/10.17502/mrcs.v10i2.577

Serrano Santoyo Arturo y Evelio Martínez Martínez, *La Brecha Digital: Mitos y Realidades,* UABC, México, 2003.

Superintendencia de institutos de formación profesional del Ministerio de Seguridad, *Cibercrimen y delitos informáticos. Apuntes para la materia,* Buenos Aires, 2022, disponible en https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

Tamarit Sumalla, Josep, "Ciberdelincuencia y victimización", *Revista de Internet Derecho y Política,* No. 22, 2016, disponible en http://journals.uoc.edu/index.php/idp/article/view/n22-tamarit/n22-tamarit-pdf-es>http://dx.doi.org/10.7238/idp.v0i22.2991>

Temperini, Marcelo Gi, "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado en XLIII Jornadas Argentinas de Informática e Investigación Operativa", *XIV Simposio Argentino de Informática y Derecho*, Buenos Aires, 2014, disponible en http://sedici.unlp.edu.ar/handle/10915/42145

Ugarte Almeida, Tamara Johanna; Nadia Acosta Ramírez y Lanny Sofía Soto Medina, "La delincuencia informática", *Revista Caribeña de Ciencias Sociales*, octubre 2021, disponible en https://www.eumed.net/rev/caribe/2015/10/delincuencia-informatica.html

Violat Avila, Marta, "El porqué de la ciberdelincuencia", 2020, disponible en https://derechodelared.com/el-porque-de-la-ciberdelincuencia/

Wall, David, *Cybercrime: The Transformation of Crime in the Information Age,* 2nd edition, Cambridge, Cambridge: Polity, 2024, disponible en https://www.wiley.com/enus/Cybercrime%3A+The+Transformation+of+Crime+in+the+Information+Age-p-9780745653532

## FUENTES LEGALES:

### *Instrumentos internacionales*

Boletín Oficial del Estado Español, BOE, "Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia", hecho en Budapest el 23 de noviembre de 2001, No. 226, de 17 de septiembre de 2010, pp. 78847 a 78896 (50 pp.), disponible en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Centro Internacional para la prevención de la criminalidad, *Informe Internacional. Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia*, 2018, disponible en https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

Conferencia de ministros de justicia de los países iberoamericanos, Secretaría General, *Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia*, 28 de mayo del 2014, disponible en https://ficp.es/wp-content/uploads/CONVENIO-CIBERDELITO-VERSION-A-LA-FIRMA.pdf

Conferencia de ministros de justicia de los países iberoamericanos, Secretaría General, *Recomendación relativa a la tipificación y sanción de la ciberdelincuencia*, 28 de mayo del 2014, disponible en https://ficp.es/wp-content/uploads/Recomendacion-Ciber-VERSI%C3%93N-A-LA-FIRMA.pdf

*Cubadebate*, "Cuba contra el delito: Detenidos autores de defraudaciones en plataformas de pago digitales", disponible en http://www.cubadebate.cu/noticias/2022/01/31/contra-el-delito-detenidos-autores-de-defraudaciones-en-plataformas-de-pago-digitales

Secretaría de Naciones Unidas, "Enfoques amplios y equilibrados para prevenir y afrontar adecuadamente formas nuevas y emergentes de delincuencia transnacional", 13º Congreso de las Naciones Unidas sobre prevención del delito y justicia penal, Doha, 12 a 19 de abril de 2015, disponible en https://www.unodc.org/documents/congress/Documentation/A-CONF.222-8/ACONF222_8_s_V1500541.pdf

## *Instrumentos nacionales*

Asamblea Nacional del Poder Popular, Ley 151/2022, "Código Penal", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 93, de 1ro de septiembre de 2022, República de Cuba, Ministerio de Justicia.

Consejo de Estado, Decreto Ley No. 370/2018, "Sobre la Informatización de la Sociedad en Cuba", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 45, del 4 de julio de 2019, República de Cuba, Ministerio de Justicia.

Consejo de Ministros, Decreto No. 360/2019, "Sobre la Seguridad de la Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 45 del 4 de julio de 2019, República de Cuba, Ministerio de Justicia.

Consejo de Estado, Decreto Ley No. 35/2021, "De las telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del espectro radioeléctrico", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, del 17 de agosto de 2021, República de Cuba, Ministerio de Justicia.

Consejo de Ministros, Decreto 42/2021, "Reglamento General de Telecomunicaciones y las Tecnologías de la Información y las Comunicaciones", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, del 17 de agosto de 2021, República de Cuba, Ministerio de Justicia**.**

Consejo de Ministros, Decreto 43/2021, "Reglamento sobre el uso del Espectro Radioeléctrico", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, de 17 de agosto de 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 105/2021, "Reglamento sobre el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, de 17 de agosto de 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 107/2021, "Reglamento para el Uso de los Servicios de Radiocomunicaciones por Satélites", *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, de 17 de agosto de 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 108/2021, "Reglamento para el Uso de los Servicios de Radiocomunicaciones por Satélites *Gaceta Oficial de la República de Cuba*, edición Ordinaria No. 92, de 17 de agosto de 2021, República de Cuba, Ministerio de Justicia.

---

Recibido: 2/7/2025
Aprobado: 25/9/2025