

Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

ARTÍCULO DE INVESTIGACIÓN

Tratamiento en el ordenamiento jurídico cubano de los delitos informáticos

Treatment of computer crimes in the Cuban legal system

Flavia Camila Regueira Gómez

flaviac@unica.cu

Universidad de Ciego de Ávila, Ciego de Ávila, Ciego de Ávila, Cuba

Celín Pérez Nájera

celinpn1973@gmail.com

Universidad de Ciego de Ávila, Ciego de Ávila, Ciego de Ávila, Cuba

<https://orcid.org/0000-0002-8964-6427>

María Victoria Sifontes Ayup

mvictoria@fpca.fgr.gob.cu

Fiscalía General de la República, Ciego de Ávila, Ciego de Ávila, Cuba

<https://orcid.org/0009-0004-8237-6163>

Recibido: 05/05/2023

Revisado: 30/06/2023

Aprobado: 10/07/2023

Publicado: 01/08/2023



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

RESUMEN

Con el desarrollo de la informática, las telecomunicaciones y la globalización del internet se produjo un incremento en la comisión de delitos informáticos. En Cuba se incrementó la incidencia de estos delitos, por lo que fue necesario el surgimiento de nuevas normas jurídicas que sancionaran las conductas delictivas y ofrecieran protección a las víctimas. El objetivo del estudio es valorar las nuevas normativas jurídicas para el tratamiento de los Delitos Informáticos en el ámbito penal-administrativo en Cuba aprobadas en el periodo comprendido entre el año 2021 al 2023. Para el desarrollo de la investigación se utilizaron métodos científicos del nivel teórico como el histórico-lógico, analítico- sintético, inductivo-deductivo y hermenéutico y del nivel empírico el análisis de contenidos. Como resultado se identificó el avance en materias de legislaciones en Cuba para el tratamiento de los delitos informáticos, en el periodo estudiado, con la aprobación de nuevas normativas jurídicas como el Decreto-Ley 35, la Resolución 105 y el Código Penal del año 2022.

Palabras Claves: Delitos informáticos; ciberseguridad; telecomunicaciones. (Tesauro Unesco).

ABSTRACT

With the development of information technology, telecommunications and the globalization of the Internet, there was an increase in the commission of computer crimes. In Cuba, the incidence of these crimes increased, making it necessary to create new legal norms to punish criminal conduct and offer protection to the victims. The objective of the study is to assess the new legal regulations for the treatment of Computer Crimes in the criminal-administrative field in Cuba approved in the period from 2021 to 2023. For the development of the research, scientific methods were used at the theoretical level, such as the historical-logical, analytical-synthetic, inductive-deductive and hermeneutic, and at the empirical level, the analysis of contents. As a result, it was identified the progress in matters of legislation in Cuba for the treatment of computer crimes, in the period studied, with the approval of new legal regulations such as Decree-Law 35, Resolution 105 and the Penal Code of the year 2022.

Keywords: Computer crimes; cybersecurity; telecommunications. (Unesco Thesaurus).



INTRODUCCIÓN

El siglo XX marcó un período de avances tecnológicos sin precedente, con la informática desempeñando un papel significativo en esta transformación. Desde la automatización de procesos en empresas y oficinas, hasta la simplificación de tareas cotidianas, en los hogares, las computadoras han proporcionado herramientas poderosas para incrementar la productividad y liberar tiempo para actividades más significativas y recreativa (Aguilar, 2011).

A medida que continuamos avanzando en el siglo XXI es fascinante contemplar cómo la informática, la tecnología y el software siguen evolucionando para abordar o transformar los desafíos actuales y futuros, la inteligencia artificial, el internet de las casas y otras tecnologías emergentes prometen impactar en la vida de manera aún más significativa. Estos avances nos recuerdan la capacidad continua de la tecnología para cambiar la vida de los individuos. Sin embargo, aparejado a esto han aparecido nuevas y variadas formas de delitos haciendo uso de este desarrollo tecnológico.

Sain (2015) señaló que la aparición de nuevas tecnologías de la comunicación, han traído consigo la posibilidad de que muchas personas realicen un uso indebido de las mismas, con el objetivo de sacar provecho. Esto comenzó a manifestarse incluso desde la época del telégrafo y el teléfono. Con la aparición de la computadora, el desarrollo del internet, así como con el incremento del número de personas con acceso a la misma, en un medio interactivo de características globales, incrementó las posibilidades de la comisión de hechos ilícitos. Los orígenes de los delitos informáticos se rastrean a partir de los años 60.

La rapidez con la que ingresó esta revolución informática a la comunidad mundial dejó en muchos casos atrasados y obsoletos a nuestros mecanismos de seguridad y control en materia de prevención de delitos, nuestra policía desprovista de los medios, de infraestructura, de estrategias modernas, del personal capacitado y de una constante actualización en lo que se refiere al aspecto comprensivo de conocimientos en materia investigativa informática tendientes a hacer frente a este nuevo reto, nos presenta un panorama de inseguridad y desprotección frente al actuar de estos modernos delincuentes cibernéticos que están situados en el mundo entero frente a un ordenador o computadora con el único propósito de sacar provecho y ventaja de sus



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

conocimientos y aplicarlos en contra de una sociedad desprotegida. (Morales, 2011, p. 1)

Ramírez & Aguilera (2009) no existe una definición universal de delito informático. Sin embargo, al consultar diferentes bibliografías coinciden en que los delitos informáticos comprenden un conjunto de conductas ilícitas para la cuales se utiliza la computadora o cualquier medio informático, y que son sancionadas por el Derecho penal.

Los delitos informáticos constituyen un verdadero problema en la actualidad, que han ido en crecimiento vertiginoso a la par del desarrollo de la informática y las telecomunicaciones. En Cuba, en los últimos años, se ha ampliado notablemente el acceso de la población a los servicios de internet, lo cual unido al uso no responsable de las redes sociales, han contribuido a que se produzca un crecimiento notable de conductas delictivas asociadas a este fenómeno.

El rápido desarrollo del internet y las comunicaciones han permitido la aparición de nuevas conductas delictivas relacionadas con la informática, lo cual nos lleva a la necesidad de que se conozca la existencia de nuevas normas jurídicas aprobadas en el periodo 2021 al 2023, encargadas de regular este tipo de delito. Con la investigación se propone no solo realizar un análisis de los principales delitos informáticos, sino también profundizar en el tratamiento que reciben estos delitos según el Ordenamiento Jurídico Cubano teniendo en cuentas las nuevas normativas puestas en vigor en los últimos años. La investigación tiene como objetivo valorar las nuevas normativas jurídicas cubanas en el ámbito penal-administrativo para el tratamiento de los Delitos Informáticos aprobadas en el periodo comprendido entre el año 2021 al 2023.

MÉTODOS

En la investigación se asumieron diferentes métodos científicos dentro de los del nivel teórico: El histórico-lógico que se utilizó para estudiar los delitos informáticos desde su surgimiento hasta la actualidad. El analítico sintético se empleó en el proceso de revisión bibliográfica con el objetivo de analizar minuciosamente y extraer de forma sintética los postulados teóricos necesarios para la solución del problema científico. El inductivo-deductivo constituyó la vía general para conducir el proceso de la investigación,



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

permitiendo analizar los referentes teóricos sobre los Delitos Informáticos. El método hermenéutico permitió realizar juicios de validez y eficacia de las normas que regulan los delitos informáticos en el ordenamiento jurídico cubano.

Del nivel empírico se utilizó el análisis de contenido: se revisaron documentos con el objetivo de determinar los datos generales relacionados con los delitos informáticos y el tratamiento de los mismos según el ordenamiento jurídico en el país, tanto bibliografías publicadas, normas jurídicas como expedientes de casos procesados por estos delitos. La novedad científica de la investigación se basa en la compilación de información acerca de un tema tan actual como son los delitos informáticos, conocimientos que pueden ser utilizados como material educativo. Permite realizar un profundo análisis y valoración aspectos relevantes relacionados con el tratamiento de los delitos informáticos según las nuevas legislaciones vigentes.

RESULTADOS

Delitos informáticos

Después de abordar de manera general los delitos, y haber hecho referencia a la ciencia de la informática, se introduce el conocimiento de los delitos informáticos, un tipo de delito de más reciente aparición y que ha venido cobrando auge en los últimos años con el desarrollo de la informática y el amplio acceso de la sociedad a la tecnología y a las redes sociales.

Los abusos informáticos abarcan cualquier incidente relacionado con la tecnología de los ordenadores en el que la víctima ha sufrido algún tipo de daño, que puede haber ocasionado graves consecuencias tanto a nivel personal como económico, mientras que el autor del delito ha obtenido o puede haber obtenido un beneficio ya sea económico, de información confidencial o de otra naturaleza, de manera intencional. Los delincuentes informáticos utilizan diversas técnicas y herramientas para llevar a cabo estos actos, aprovechándose de las vulnerabilidades en los sistemas informáticos y las redes (Parker, 1976).



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

Cuando se habla de delitos informáticos se refiere a un conjunto de comportamientos que constituyen delitos penales que deben tener un tratamiento legal ya que tienen como objeto causar daños a terceras personas, ocasionando lesiones y en algunos casos pérdidas de bienes jurídicos. Se habla de actividades ilícitas que se cometen utilizando tecnologías de la información y las comunicaciones como computadoras, redes y dispositivos electrónicos, El entorno donde ocurre estos delitos se conoce como ciberespacio (Fuente et al., 2018).

Otro concepto respecto a lo que se entiende por delitos informáticos es:

Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en la actividad informática. (Camacho, 1987, p.25)

Características principales de los delitos informáticos

La dificultad en la detección es una característica clave en esta actividad delictiva que está muy relacionada con su carácter transnacional, pues esto puede impedir que se conozca desde donde se produjo la acción delictiva. El reconocimiento de estos delincuentes representa todo un desafío debido a la naturaleza del internet como un entorno dinámico y accesible para muchos, su alcance complejidad la gran cantidad de dispositivos conectados, hace que la identificación de los delincuentes informáticos que en muchos casos poseen conocimientos técnicos avanzados que les permite ocultar su rastro con relativa facilidad sea un verdadero reto (Artavia, 2017).

Definitivamente uno de los rasgos fundamentales del delito informático es su dependencia del sistema informático según López y Torres (2010), “para su existencia necesita del uso de un ordenador generalmente con conexión a internet” (p. 36). Además del uso de ordenadores es importante destacar que los delitos informáticos también pueden involucrar otros dispositivos y sistemas conectados a internet como teléfonos, servidores, entre otros.

Otra de las características prominentes de los delitos informáticos es su fuerte orientación hacia el beneficio económico para sus autores, los individuos que realizan estos actos



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

comoackers, crackerso reakers, generalmente buscan obtener algunos tipos de ventajas, generalmente de manera financiera. Algunas de las formas más comunes en las que los delincuentes informáticos buscan lograr ganancias económicas incluyen fraude cibernético, clonación de tarjetas de créditos, robo de datos entre otras (Artavia, 2017). Este delito tiene carácter transnacional “nos encontramos frente a un hecho delictivo que puede cometerse en un país y tener sus efectos perjudiciales en otro u otros, siendo que la acción y el efecto pueden estar separados por miles de kilómetros” (López y Torres, 2010, p. 37).

Tipos de delito informáticos

El término ciberterrorismo se refiere en esencia a una forma de terrorismo en la que no se requiere la presencia física de los individuos para cometer actos de violencia o provocar un impacto a gran escala. En lugar de depender del contacto directo, como en el caso de los atentados con bombas o secuestros, el ciberterrorismo utiliza las redes informáticas y los sistemas de información como su principal medio de acción. Esta particularidad es la que lo hace tan distintivo a la vez desafiante desde el punto de vista de la seguridad y el derecho (Sánchez, 2021).

Según Rangel (2005) se entiende, “como la sucesión de actos para infundir terror utilizando medios informáticos, con el fin de lograr un cambio radical en el orden constitucional de un Estado” (p. 122).

Otro concepto acertado es:

Cualquier acto realizado a través de tecnologías de información que pueden lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción del soporte tecnológico de cualquiera de sus infraestructuras fundamentales. (Subijana, 2008, p. 173)

Este tipo de terrorismo reconoce a internet como su principal canal de ataque. La disponibilidad generalizada, la accesibilidad de la red mundial permite a los actores malintencionados llevar a cabo sus actividades con relativa facilidad y un costo relativamente bajo. La presencia universal del internet como un medio para la



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

comunicación, el intercambio de información, la realización de transacciones lo convierte en un blanco efectivo para aquellos que buscan perpetrar ataques cibernéticos por motivos terroristas (Rangel, 2005).

El surgimiento del cyberbullying es un claro ejemplo de cómo las tecnologías de la información y la comunicación han dado lugar a nuevas formas de agresión y violencia, particularmente entre los jóvenes. Este fenómeno tiene el propósito de intimidar, acosar o dañar a otra persona, buscando generar un impacto negativo en la víctima usando como instrumento las tecnologías. Este tipo de comportamiento puede incluir la difusión de rumores maliciosos, la publicación de comentarios ofensivos, entre otros (Broll, 2016, como se citó en Neyra, 2021)

El concepto de cyberbullying se entiende como:

el uso de algunas Tecnologías de la Información y Comunicación como el correo electrónico, los mensajes del teléfono móvil, la mensajería instantánea y las Web personales- para manifestar comportamientos vejatorios y/o difamatorios de un individuo o un grupo, que deliberadamente y de forma repetitiva y hostil, pretendía dañar otro. (Belsey, 2005, como se citó en Sabater & López, 2015, p. 4)

Este tipo de acoso comparte similitudes con otras formas de acoso como su intencionalidad, su premeditación, y la dinámica de poder entre el agresor y la víctima. Sin embargo también presenta características que lo distinguen de otras formas de acoso presencial y directo, lo que resalta la importancia de comprender y abordar esta polémica de manera específica. Entre sus particularidades está; que exige el dominio y uso de las tecnologías, es una forma de acoso indirecto; pues a diferencia del acoso presencial este ocurre a través de plataformas en línea lo que dificulta la identificación del agresor, además se caracteriza por el desamparo legal; porque aunque se puede cerrar la web inmediatamente se puede abrir otra y su naturaleza pública y de rápida difusión que hacen que los contenidos se propaguen rápidamente amplificando su impacto (Hernández & Solano, 2007).

Todo lo anteriormente expuesto hace reflexionar en lo devastador que puede llegar a ser este fenómeno en la autoestima y la salud mental sobre todo en los adolescentes y jóvenes que lo experimenten. La exposición a este tipo de violencia y comportamientos



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

hostiles llegan a generar una pesada carga psicológica que afecta profundamente la confianza en sí mismo y la percepción de su valía como individuo. Puede llevar a situaciones de estrés, ansiedad e incluso aislamiento de la sociedad, lo que a su vez puede inhibir la capacidad de los jóvenes para interactuar socialmente, participar en actividades educativas, deportivas, culturales y disfrutar de una vida equilibrada y saludable.

Es fundamental reconocer el impacto del cyberbullying en la salud mental de los jóvenes y asegurar que se les brinde el apoyo necesario para sobrellevar estas situaciones sobre todo por parte de las familias que es un pilar fundamental. Abordar estas complejidades requiere un enfoque multidisciplinario que incluya a educadores, profesionales de la salud mental, legisladores y la sociedad en general.

La clonación de tarjetas normalmente se produce cuando los delincuentes utilizan dispositivos especializados para copiar la información de la banda magnética de una tarjeta. Esta información se coloca en una tarjeta falsificada y puede ser utilizada para efectuar compras no autorizadas o para realizar retiros de efectivo fraudulento. Además, en muchos casos los criminales recurren al denominado *skimming* que consiste en instalar dispositivos ilegales conocidos como *skimmer* en cajeros automáticos o terminales de pago, los cuales capturan la información de la tarjeta de la víctima sin su consentimiento. Su amplitud geográfica, pues puede ocurrir tanto en cajeros automáticos como centros comerciales, lo convierten en un delito particularmente preocupante (Roldan et al., 2017).

La metodología que utilizan los delincuentes para realizar el robo de identidad permite que los usuarios no se percaten de las anomalías o fechorías empleadas para robar datos del plástico, muchas veces hurtan únicamente los datos asociados al plástico, sin necesidad de llegar a clonar la tarjeta.
(Martínez, 2021, p. 16)

Además de los skimmer existen otras variantes de dispositivos utilizados en este tipo de delitos, como cámaras ocultas o teclados falsos que capturan los PIN de los usuarios, permitiéndoles a los delincuentes tener acceso completo a las cuentas de las víctimas. Dado el impacto que tiene este fenómeno es crucial estudiar y comprender a fondo los mecanismos que llevan a la clonación de tarjetas, así como implementar medidas



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

eficaces para evitar que ocurran. Desde leyes que penalicen duramente estas prácticas fraudulentas, hasta la aplicación de tecnologías de seguridad más avanzadas, estos dos factores son fundamentales para mitigar el problema.

El fraude, es de hecho un delito sumamente creativo que requiere astucia y perspicacia, lo que lo convierte en un desafío difícil de evitar. Los delincuentes que cometen fraude están constantemente buscando nuevas formas de engañar a las personas y los sistemas, utilizando tecnologías avanzadas y métodos sofisticados de manipulación de datos. El panorama en constante evolución del fraude digital significa que tanto individuos como organizaciones deben estar en alerta constante para protegerse contra estas amenazas en evolución. De no tomarse las debidas precauciones es posible vivir la desagradable experiencia de ser víctima de fraude cibernético que puede causar pérdidas significativas en la economía (Aguilar, 2011).

Después de analizar conceptos emitidos por diferentes conocedores del tema respecto a lo que entienden por fraude cibernético se puede decir que es una acción intencional y engañosa que se realiza utilizando medios tecnológicos para lograr que otra persona haga o dejen de hacer algún tipo de actividad que conlleve a la pérdida de un bien. Se habla de un desafío en constante evolución que requiere respuestas innovadoras y colaborativas.

El robo de identidad digital, sin dudas, se ha convertido en una preocupación significativa en el ámbito de la ciberseguridad. A medida que la sociedad se vuelve cada vez más dependiente de la tecnología digital, los delincuentes han aprovechado las vulnerabilidades para perpetrar ataques dirigidos al robo de identidad personal y empresarial. A pesar de las dificultades en la obtención de estadísticas que demuestren en forma efectiva y precisa el auge de esta actividad delictiva. Numerosos estudios han evidenciado el crecimiento exponencial de esta forma de delito (Borgello & Temerini, 2012).

Al respecto, puede afirmarse que no existe un único y homogéneo concepto de robo de identidad; sin embargo de todas las conceptualizaciones existentes, pueden observarse determinados elementos comunes. En términos generales el robo de identidad tiene lugar cuando una persona utiliza



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

la información personal de otro individuo ara realizar compras, solicitar restamos, obtener un trabajo; en definitiva: hacerse pasar por alguien que verdaderamente no es. (Monastersky & Salimbeni, 2012)

El daño causado por suplantación de identidad digital va más allá de las pérdidas económicas inmediatas. La injuria a través de las redes que atenta contra el honor y la reputación de la víctima es uno de los impactos más profundos, duraderos de este tipo de delito. La suplantación de identidad puede causar un impacto social, psicológico, moral significativa en la vida de la persona afectada. El hecho de que un tercero pueda utilizar la identidad digital de la víctima, robando nombres de usuario, contraseñas y acceso a cuentas en el correo electrónico, redes sociales, foros y otras plataformas representa una invasión en la vida personal, que puede llevar a un sentimiento de vulnerabilidad, una violación de la privacidad y una pérdida de control sobre su propia representación en línea (Borgello & Temerini, 2012).

Las víctimas de la suplantación de identidad digital pueden experimentar una combinación de efectos emocionales, como ansiedad, estrés, vergüenza, frustración e incluso temor especialmente si sus datos personales se utilizan con el fin de cometer otros actos delictivo difundir informaciones fraudulentas o dañinas. Además el impacto emocional psicológico puede afectar la vida diaria de la víctima tanto en el ámbito laboral como en el personal.

Nuevas normativas jurídicas en materia de telecomunicaciones en Cuba

En los últimos años Cuba pone en vigor un grupo de nuevas normativas en materia de telecomunicaciones que representan un paso significativo para regular y adaptarse a los avances tecnológicos en el país. Este tipo de actualización legal es crucial para asegurarse de que las leyes estén alineadas con el rápido desarrollo tecnológico y la evolución de los servicios de telecomunicaciones.

Es realmente esencial que las actualizaciones en el marco jurídico estén alineadas con los objetivos del desarrollo político, económico social del país. Por primera vez "el país contará con una norma jurídica donde se asocien incidentes de ciberseguridad y tipificaciones que superen los límites de lo tecnológico "(Domínguez, 2021, como se citó



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

en Figueredo, 2021). Esto constituye un avance significativo en el ámbito legal de seguridad en el país. Esta medida señala un reconocimiento de la importancia de la ciberseguridad en un contexto cada vez más digitalizado.

La creación de una normativa que aborde los incidentes de ciberseguridad va mucho más allá de preocupaciones meramente tecnológicas. Esto sugiere un entendimiento más profundo de los riesgos que los incidentes de ciberseguridad representan, y de cómo estos pueden afectar diversos aspectos de la sociedad, la economía y la seguridad nacional.

Decreto Ley No 35, de las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y del Uso del Espectro Radioeléctrico

El Decreto-Ley 35 fue publicado en la Gaceta Oficial de la República el 1 de agosto del año 2021, esta regulación forma parte de la actualización del marco jurídico en materia de telecomunicaciones en Cuba, en la misma se dicta: "Este Decreto-Ley es aplicable a las relaciones jurídicas en la esfera de las telecomunicaciones/TIC y en el uso del espectro radioeléctrico, con las personas naturales y jurídicas que utilicen estos recursos y sus servicios" (Decreto-Ley 35, 2021, Artículo 4).

El Decreto-Ley No 35 es la primera norma jurídica de rango superior aprobado en nuestro país sobre los servicio de telecomunicaciones, las TIC el uso del espectro radioeléctrico, a la que se le asigna una mayor jerarquía e importancia por su transversalidad en los procesos de la sociedad, lo que permite una mayor coherencia y ordenamiento del marco regulatorio existente.

(López, 2021 como se citó en Figueredo, 2021)

Esto enfatiza la importancia histórica y la naturaleza integral de este Decreto en relación con el servicio de telecomunicaciones y el uso del efecto radioeléctrico en Cuba. La caracterización del Decreto- Ley como transversal en los procesos de la sociedad resalta su naturaleza integral y su impacto generalizado en diversos aspectos de la vida y la actividad social, económica y gubernamental en el país. La elevada importancia otorgada a esta normativa está en sintonía con la evolución tecnológica su impacto sobre la sociedad, demuestra una respuesta proactiva estratégica en la regulación de estas áreas fundamentales.



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

EL Decreto-Ley No 35 refleja múltiples objetivos y enfoques claves en el ámbito de las telecomunicaciones en Cuba entre ellas la utilización de las telecomunicaciones como un instrumento para la defensa de la Revolución subraya la importancia estratégica de las telecomunicaciones en el contexto de la seguridad estabilidad del país, enfatizando su papel en la promoción de los valores y objetivos revolucionarios. El impulso del uso de las telecomunicaciones, la priorización de redes de banda ancha que protejan los intereses de los ciudadanos garantizando la igualdad de acceso, seguridad, privacidad secreta en las comunicaciones promoviendo de ese modo el desarrollo económico, político social del país. Se enfatiza en elevar la ciberseguridad contra amenazas internas y externas. Refiere la necesidad de satisfacer las necesidades del Estado, el Gobierno la relacionadas con la Seguridad y la Defensa Nacional, entre otras (Decreto-Ley No 35, 2021, Artículo 1).

Con este Decreto-Ley se establecen un grupo de deberes que los usuarios de los servicios de telecomunicaciones/TIC deben cumplir al hacer uso de ellas para evitar con sus acciones causar un daño a una tercera persona y de esta forma incurrir en un delito informático.

Impedir que los servicios de telecomunicaciones/TIC se utilicen para atentar contra la Seguridad y el Orden Interior del país, transmitir informes o noticias falsas, o en acciones dirigidas a ocasionar afectaciones o perjuicios a terceros y como medio para cometer actos ilícitos. (Decreto- Ley No 35, 2021, Artículo 15)

El uso de las tecnologías para difundir desinformación es una preocupación para el gobierno cubano, dado que el impacto de estas acciones puede tener efectos importantes en la estabilidad política. Estados Unidos ha utilizado este medio para sembrar confusión en el pueblo cubano y fomentar la inestabilidad política.

no usar el servicio para realizar acciones o transmitir información ofensiva o lesiva a la dignidad humana; de contenidos sexuales, discriminatorios; que genere acoso; que afecte la intimidad personal y familiar o la propia imagen y voz; la identidad, integridad y el honor de la persona; la seguridad colectiva, el bienestar general, la moralidad pública y el respeto al orden público. (Decreto-Ley No 35, 2021, Artículo 15)

Por supuesto, este enfoque es fundamental para fomentar un entorno digital respetuoso y seguro. Evitar el uso de los servicios tecnológicos para transmitir información ofensiva



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

discriminatoria acusadora o que viole la intimidad personal, es esencial para promover relaciones sanas y respetuosas en línea y para crear un ambiente seguro donde se valore el respeto mutuo, la dignidad humana y la convivencia armoniosa. Estos son pasos importantes para fomentar una cultura en la que se promueve el bienestar el respeto para todos los individuos que participan en el entorno digital.

Resolución 105, Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad.

La Resolución 105 representa un paso significativo en aras de la protección de los derechos individuales en el ciberespacio. Esta aplicación no solo refleja una adaptación a las necesidades actuales, sino que también permite una mayor protección de los derechos de los ciudadanos, al tipificar los incidentes que pueden amenazar al individuo, a la tranquilidad ciudadana, al desarrollo de la sociedad en todas sus esferas.

Esta Resolución le brinda protección tanto a las personas naturales como jurídicas en la medida de lo posible, tomando en consideración la existencia de pruebas, lo cual tiene como objetivo prevenir y detectar posibles amenazas enemigas, que puedan ocurrir en el ciberespacio y responder de manera oportuna neutralizando o minimizando las posibles consecuencias. Busca una respuesta colaborativa entre los organismos involucrados en la seguridad de las TIC y la defensa del Ciberespacio Nacional, utilizando un término común para clasificar estos incidentes así lograr una comprensión clara una respuesta efectiva (Resolución 105, 2021, Artículos 1,2).

Por medio de la Resolución 105 se describe de manera detallada las etapas de actuación ante un incidente de ciberseguridad, estableciendo acciones obligatorias en cada una de estas fases. En la etapa uno de prevención protección, se llevan a cabo acciones que buscan evitar incidentes cibernéticos, estas acciones se orientan a la reducción de vulnerabilidades y el fortalecimiento de las defensas cibernéticas. En la etapa dos de detección, evaluación y notificación, se busca identificar de manera rápida y efectiva la presencia de una amenaza cibernética, evaluar su impacto en la seguridad y notificar de manera oportuna. En la etapa tres de investigación, se centra en el esclarecimiento de



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

indicios. En la etapa cuatro de mitigación recuperación, en ella se implementan acciones para remediar los daños causados y mitigar las vulnerabilidades que permitieron el incidente (Resolución 105, 2021, Art 6).

Es importante destacar que la clasificación y caracterización de los incidentes de Ciberseguridad son herramienta esenciales para la gestión efectiva de la seguridad de la información. Al comprender la naturaleza de los incidentes y evaluar su nivel de peligrosidad, las organizaciones pueden tomar medidas proactivas para prevenir y mitigar posibles riesgos.

Otras norma de menor relevancia que brindan seguridad al espacio cibernético

Otra normativa que fue aprobada en Cuba en el año 2021, fue el Decreto 42 Reglamento General de Telecomunicaciones y las Tecnologías de la Información y la Comunicación. Con él se amplía, se esclarece y proporciona orientación adicional sobre las disposiciones establecidas en el Decreto Ley No 35 analizado anteriormente. Además ofrece información y reglamentaciones más detalladas. Hace referencia a los diferentes servicios de telecomunicaciones/TIC a los que se les aplica este Reglamento, puntualizando que los nuevos servicios de telecomunicaciones que surjan en lo adelante también les son aplicables tanto este Reglamento como sus disposiciones normativas complementarias y que si se tratan de servicios públicos requiere autorización por el Ministerio de Telecomunicaciones (Decreto 42, 2021, Artículos 2, 3, 4,5).

"El Ministerio de Comunicaciones establece las modalidades de procedimientos alternativos de llamadas internacionales que no se permiten que se utilicen en el país"(Decreto 42, 2021, Artículo 12). Esta disposición puede estar orientada a regular aquellas prácticas o métodos de comunicación internacional que, por diversas razones podrían considerarse inapropiadas o perjudiciales para la seguridad, la economía y otros aspectos relevantes ara el país. La regulación de los procedimientos alternativos de llamadas internacionales, también podría estar relacionada con la protección de las redes de comunicación, la privacidad de los ciudadanos, la lucha contra el fraude, la seguridad nacional, entre otros aspectos. Al establecer modalidades específicas controlar el uso de



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

procedimientos alternativos de llamadas internacionales, el Ministerio de Comunicaciones busca asegurar un uso adecuado y seguro de las comunicaciones internacionales en el país.

En el Decreto 42 (2021) se establece el momento en el cual se puede realizar el inicio de la acción administrativa que es a partir de momento en que se identifica al comisor. En el mismo se subraya que las sanciones u otras medidas administrativas no excluyen la posibilidad de enfrentar otra forma de responsabilidad, como la penal o la civil, dependiendo de la gravedad de las infracciones cometidas (Artículos 74, 75).

Por otra parte, se establece el Decreto 43 Reglamento sobre el uso del espectro radioeléctrico

El presente Decreto tiene por objeto establecer las disposiciones reglamentarias principales en materia de utilización del espectro radioeléctrico que complementan lo dispuesto en el Decreto 35 “De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y del uso del Espectro Radioeléctrico”, de 13 de abril de 2021. (Decreto 43, 2021, Artículo 1)

Es interesante ver como el Decreto amplía su alcance no solo a disposiciones sobre el uso del espectro radioeléctrico y los servicios que utiliza, sino también a la evolución de las tecnologías de las comunicaciones, su relación con personas naturales y entidades jurídicas. Este enfoque más amplio reconoce la importancia de adaptarse a los cambios tecnológicos y a las nuevas formas de comunicación inalámbrica, cómo estas afectan a diferentes actores en la sociedad.

También, la Resolución 107 Reglamento para el uso de los servicios de radiocomunicaciones por satélites aborda específicamente el régimen jurídico de radiocomunicaciones por satélites. Estos servicios son fundamentales en la actualidad, ya que implican la transmisión y recepción de ondas radioeléctricas a través de satélites para propósito de telecomunicaciones. Los servicios de radiocomunicaciones por satélites abarcan un amplio espectro de aplicación tecnologías que van desde servicios móviles por satélites, servicios fijos de satélites, servicios de radio difusión por satélites, entre otros (Resolución 107, 2021, Artículo 1).



Tratamiento jurídico de los Delitos Informáticos desde el Código Penal Cubano.

Según el Código Penal Cubano (2022) en relación con el delito de desórdenes públicos

Quien, a sabiendas, difunda noticias falsas o predicciones maliciosas con el objetivo de causar alarma, descontento o desinformación en la población, o para provocar alteraciones del orden público, incurre en sanción de privación de libertad de uno a tres años o multa de trescientas a mil cuotas, o ambas. (Artículo 266.1)

Si, para la ejecución de los hechos previstos en el apartado anterior, se utilizan las redes sociales o medios de comunicación social en los espacios físico y digital, la sanción es de privación de libertad de dos a cinco años o multa de quinientas a mil cuotas, o ambas. (Artículo 226.2)

En el Código Penal cubano se resalta la gravedad de utilizar las redes sociales o medios de comunicación social en la difusión de noticias falsas o predicciones malintencionadas. La inclusión de sanciones más estrictas para tales acciones cuando se llevan a cabo a través de medios digitales subraya la importancia de controlar la difusión de informaciones engañosas en el entorno en línea dado el alto impacto perjudicial que puede tener pues la información se difunde con una rapidez inigualable.

Esto es un ejemplo claro de cómo los marcos legales buscan mantenerse al día con los avances tecnológicos y la evolución de los medios de comunicación, adecuando sus disposiciones para abordar la complejidad del entorno digital en un tema tan delicado como este pues está estrechamente vinculado con la libertad de expresión.

La difusión de hechos falsos que dañen la reputación de una persona puede tener efectos graves en la vida personal y profesional, provocando una angustia emocional que puede llevar a la persona a sentirse vulnerable, ansiosa e incluso con un alto grado de depresión.

Aun cuando en el Código Penal cubano puede no definir específicamente el término de ciberterrorismo, si sanciona a aquellos que facilitan la comisión de estos actos que afectan la seguridad informática, la estabilidad del estado y la integridad de la sociedad.



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

Haciendo referencia al uso de medios, equipos o programas que puedan dañar soportes informáticos o programas de emergencia, de seguridad nacional o internacionales, o que con el uso del internet comercialice programas capaces de causar estos daños (Código Penal, 2022, Artículo 168).

CONCLUSIONES

La investigación revela que, durante el período 2021-2023, Cuba ha respondido de manera proactiva al problema de los Delitos Informáticos mediante la implementación de nuevas normativas jurídicas. El enfoque en la regulación de las telecomunicaciones y la aprobación del Código Penal actual demuestran un esfuerzo significativo por parte de las autoridades cubanas para adaptar el marco legal a la creciente informatización de la sociedad, lo que sugiere una respuesta adecuada a los desafíos actuales en el ámbito penal-administrativo.

Se destaca la importancia de las normativas implementadas en el año 2021, como el Decreto Ley No 35 y la Resolución 105, que abordan específicamente la difusión de noticias falsas y la ciberseguridad. Estos documentos legales evidencian un enfoque estratégico para contrarrestar las amenazas digitales, resguardando así a la sociedad cubana de posibles ataques y delitos informáticos.

La aprobación del Código Penal en 2022, aunque no incluye un título específico para los delitos informáticos, constituye un paso adelante al integrar términos como "redes sociales" en figuras delictivas y dedicar un título exclusivo a la protección de las telecomunicaciones y servicios vinculados a la tecnología de la información. Este avance refleja un esfuerzo por modernizar y fortalecer la legislación cubana en respuesta a la complejidad de los delitos informáticos, ofreciendo así una mayor protección a los ciudadanos y una base jurídica más sólida para abordar estos fenómenos en evolución. Se recomienda para futuras investigaciones profundizar en relación con la Resolución 105, Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad, específicamente en las acciones a ejecutar en las diferentes etapas ante un incidente de ciberseguridad.



REFERENCIAS

- Aguilar Olguin, C. (2011). *El delito de fraude cibernético sus implicaciones jurídicas en México*. [Tesis de Licenciatura, Universidad Nacional Autónoma de México] .
- Antúnez Sánchez, A. F y Soler Pellicer, Y . (2013). La auditoría a las tecnologías de la informática. Relación del derecho y la informática jurídica. *Derecho y Cambio Social*, 10(32), 30.
- Arroyo Chacon, J. I. & Francisco Monge, J. (2016). El papel del estado frente al espectro radioeléctrico como bien demanial. *Derecho y comunicación*
- Artavia Solano, M.B. (2017). *Pornografía infantil en la red su connotación como delito informático* . [Tesis de Licenciatura Universidad Latinoamericana de Ciencias Tecnología]
- Asamblea General de las Naciones Unidas. (2000). Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños Pornografía. Naciones Unidas.
- Barrera López, J. (1996). La importancia de la informática en la educación. Universidad de Lasalle.
- Borgherillo. C. & Temperini. M. (2012). Suplantación de Identidad Digital como Delito Informático en Argentina. Simposio Argentino de Informática y Derecho.
- Camacho Losa, L. (1987). *El delito informático*. Editorial Ilustrado. Madrid.
- Cortés Borrero, R., Ballén Rojas, J.A & Duque Montes, J.J. (2015). La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*.
- Espinoza Céspedes. (2020). El Sistema Peruano de Información Jurídica: un aporte eficiente a la revolución digital, y el trabajo en un contexto de sistematización jurídica. *Revista del Instituto de Ciencias Jurídicas de Puebla*, 14(45), 27-53.
- Figueredo Reinaldo, O. (2021). *Cuba actualiza marco jurídico en materia de telecomunicaciones tipifica incidentes de ciberseguridad*
<http://www.cubadebate.cu>



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

- Fuentes Marrufo, T. E., Mazún Cruz, R. & Cancino Mendaz, G. (2018). Perspectiva sobre los delitos informáticos: Un punto de vista de estudiantes del Tecnológico Superior Progreso. *Revista Advances in Engineering and innovation*. 2(4), 1-8.
- Gobierno de España. (2011). Plan de acción contra la explotación sexual de la infancia y la adolescencia. <http://www.mdsocialesa2030.gob.es>.
- Hernández Prados, Ma. Á., & Solano Fernández, I. Ma. (2007). Cyberbullying, un problema de acoso escolar. *Revista Iberoamericana de Educación a Distancia*, 10(1), 17-36.
- Kaiser, G. (1978). *Una Introducción a sus Fundamentos científicos*. Espasa Calpe.
- Lemaitre Picado, R. (2017). Delitos penales de pornografía infantil en Costa Rica. *Revista Firma*, 16(16), 20-21.
- López Vargas, J. A. & Torres Granados, M. (2010). *Problemática del delito informático: Hacia una necesidad de regulación internacional*. Costa Rica San José.
- Loredo González, J.A. & Ramírez Granados, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. *Revista Celerinet*, 44-51.
- Martínez Ralón, M.A. (2021). Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados. *Revista Científica Dialogo Forense*, 2(4).
- Mayer Lux, L., & Oliver Calderón. (2020). El delito de fraude informático: concepto y delimitación. *Revista chilena de derecho y tecnología*, 9(1), 151-184.
- Mayo, M. C. (1991). *Informática jurídica*. Jurídica de Chile.
- Morales Cuba, R. A. (2011). *Fundamentos jurídicos sociales para reglamentar la creación y capacitación de la policía especializada en informática para la represión y prevención de los delitos inforáticos*. Tesis en Licenciatura, Universidad Mayor de San Andrés.
- Miró Linares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons.
- Monastersky. D. & Salimbeni. M. (2012). Introducción al Robo de Identidad. [Archivo PDF]. <https://dl.droboxusercontent.com>



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

- Moscoso Delgado, J. (1981). *Introducción al Derecho*. Juventud.
- Neyra Castilla, O.M. (2021). *Autoestima, auto concepto y cyberbullying en estudiantes del primer ciclo de una universidad privada del distrito de los Olivos*. [Doctorado en Psicología, Universidad Cesar Vallejo].
- Nieto Huertas, L. (2003). El estado del Arte de la Seguridad Urbana. *Revista de Ciencias Sociales del Instituto Universitario de Investigación Ortega y Gasset*.
- Padilla Segura, J. (1991). *Informática jurídica*. I.P.N, México
- Parker, D. B. (1976). *Crime by computer*. Charles Scribners Sons.
- Ramírez Bejerano, E., & Aguilera Rodríguez, A.R. (2009). Los delitos informáticos. Tratamiento internacional. *Revista Caribeña de Ciencias Sociales*. <http://www.eumed.net/rev/caribe>
- Rangel Velásquez, E. (2005). *Terrorismo Informático y su Perspectiva Jurídica*. [Tesis de Grado Universidad Mayor de San Andrés].
- Ranieri, S. (1997). *Derecho Penal: Teoría del Delito*. [Tesis de Grado Universidad Nacional Autónoma de México].
- Rincón Ríos, J. (2015). *El delito en la cibersociedad y la justicia penal internacional*. [Tesis Doctoral, Universidad Complutense de Madrid].
- Roldan, L. Ma., Rincón, L. Ma., & Taborda, A. (2017). *Clonación de Tarjetas de Crédito*. [Trabajo de Grado, Tecnológico de Antioquia Institución Universitaria Facultad de Ciencias Administrativas y Económicas. Medellín].
- Rubio Vidal, J. E. (2005). Importancia de la informática y las nuevas tecnologías en la educación. *XVIII Jornadas de Pedagogía Social. ¿Construimos alternativas educativas desde los movimientos sociales?, p 375-377*.
- Sabater Fernández, C., López Hernández, L. (2015). Factores de Riesgo en el Cyberbullying. Frecuencia y exposición de los datos personales en Internet. *Revista International Journal of Sociology of Education*, 4(1), 1-25.
- Saín, G. (2015). Evolución histórica de los delitos informáticos. *Revista Pensamiento Penal*.



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

- Sánchez Gill, L. M. (2021) Repensando el concepto de ciberterrorismo. Universidad de Salamanca. Instituto Español de Estudios Estratégicos. Documento Opinión.
- Serrano Maíllo, A. (2008). *Introducción a la Criminología*. Editorial Dykinson.
- Subijana Zunzunegui, I.J. (2008). El ciberterrorismo: una perspectiva legal judicial. *Revista Eguzkilore del Instituto Vasco de Criminología* (22), pp169-187.
- Téllez Valdez, J. (1996). *Derecho informático*, Ed. McGraw Hill.
- Valdivia Zapata, J.A. (2023). *La eficacia de la persecución penal del delito de fraude informático en el Perú*. [Tesis de Grado, Universidad Tecnológica de Perú].

LEGISLACIONES

- Código Penal. Ley 151 de 2022 Gaceta Oficial No. 93 Ordinaria de 1ro de septiembre de 2022. Cuba.
- Constitución de la República 2019. Gaceta Oficial No 5 Extraordinaria de 10 de abril de 2019.
- Decreto-Ley 35 de 2021. De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del Espectro Radioeléctrico. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021,
- Decreto 42 de 2021. Reglamento General de Telecomunicaciones y las Tecnologías de la Información y la Comunicación. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021.
- Decreto 43 de 2021. Reglamento sobre el uso del Espectro Radioeléctrico. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021.
- Resolución 105 de 2021. Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021.
- Resolución 107 de 2021. Reglamento para el uso de los Servicios de Radiocomunicaciones por Satélites. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021.



Flavia Camila Regueira Gómez; Celín Pérez Nájera; María Victoria Sifontes Ayup

Resolución 108 de 2021. Reglamento de Interconexión, Acceso e Instalaciones Esenciales de Redes de Telecomunicaciones. Gaceta Oficial No. 92 Ordinaria de 17 de agosto de 2021, Ministerio de Comunicaciones,

