EL DELITO INFORMÁTICO EN EL MARCO JURÍDICO COLOMBIANO Y EL DERECHO COMPARADO: CASO DE LA TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

MONOGRAFÍA DE INVESTIGACIÓN

JESÚS ARLES GAMBA VELANDIA

DIRECTOR:

Dr. ALBERTO SUÁREZ SÁNCHEZ

UNIVERSIDAD EXTERANDO DE COLOMBIA

FACULTAD DE DERECHO

MAESTRÍA EN JUSTICIA Y TUTELA DE LOS DERECHOS CON ÉNFASIS EN CIENCIAS PENALES Y CRIMINOLÓGICAS

BOGOTÁ, D.C

2019

Contenido

Índice de Tablas

INTRODUCCIÓN

La globalización, las tecnologías de la información y la comunicación TIC, el Internet y las redes sociales, son algunas de las manifestaciones más destacadas que actualmente inciden en las relaciones económicas de los países, las organizaciones y la sociedad civil en general. Sin embargo, a la par con el progreso tecnológico, la interacción comunicativa permanente a través de medios informáticos, el incremento en la productividad de las empresas debido a la innovación tecnológica y el estrechamiento de relaciones comerciales, económicas, políticas y culturales entre naciones, también está latente la amenaza permanente por parte del crimen organizado trasnacional - COT expresado en el ciberdelito en todas sus manifestaciones: terrorismo, narcotráfico, trata de personas, blanqueo de capitales, entre otros, lo cual obliga a la comunidad internacional, los organismos multilaterales, los Estados, las empresas y la sociedad en general, establecer estrategias comunes para combatir los riesgos y castigar la cibercriminalidad[1].

En este contexto, existe un gran desafío para las legislaciones internas de los países y el marco internacional en torno a legislar sobre las causas punibles del ciberdelito, dada la diversidad de medios que originan su comisión frente a la pluralidad y diversidad de bienes jurídicos afectados, la necesidad de establecer

[1] BARRIOS A., M. Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015. España: Editorial Reus S.A., 2018.

precisiones desde el punto de vista criminológico, dogmático y político criminal de política legislativa[2].

Frente a esta problemática, muy frecuente en el sistema financiero, la presente investigación monográfica aborda el estudio sobre el delito informático en el marco jurídico colombiano y el derecho comparado en respuesta a la pregunta problema: ¿Cómo analizar el delito informático dentro del marco jurídico colombiano: el caso de la transferencia no consentida de activos y su tratamiento en el derecho comparado?

Para el efecto, se plantearon varios objetivos específicos relacionados con contextualizar la tipificación del delito informático y su tratamiento jurídico en el ámbito internacional por parte de algunos países y organismos internacionales, caracterizar el delito informático en Colombia dentro del actual marco jurídico legal y su consideración en el derecho comparado y examinar las características de la Transferencia no consentida de Activos como caso de delito informático y su tratamiento en el Código Penal Colombiano.

La metodología empleada para su desarrollo de este estudio, estuvo enmarcada dentro de las características de investigación cualitativa, de carácter

[2] ROMEO C., Carlos María. De los delitos informáticos al cibercrimen: En Universitas vitae homenaje a Ruperto Núñez Barbero. Ediciones Universidad de Salamanca, 2014.

exploratoria, bajo un enfoque analítico-interpretativo de revisión documental[3] para caracterizar el estado de la cuestión en la temática y ámbito del marco del derecho comparado, su tratamiento doctrinal y jurídico legal, a partir de consultas en las principales bases de datos científicas tales como como Scopus, Redalyc, Scielo, Google Scholar, Ebsco, Proquest, V-lex, utilizando palabras clave: ciberdelito, delito informático, legislación delito informático, estafa informática, entre otros.

La justificación de llevar a cabo esta investigación se planteó debido a la necesidad de contribuir a la consolidación y referenciación sobre la tipificación y tratamiento jurídico-legal por parte de organismos internacionales generadores de *soft law* en la materia y los avances de *hard law* por parte de países de manera individualizada y comunidad de países ante diferentes tratados y acuerdos comerciales de carácter bilateral y multilateral. Igualmente, la proliferación de diferentes tipologías de ciberdelitos, dado el auge del uso del Internet y las TICs en todos los ámbitos de la sociedad global y la existencia de vacíos teóricos y uniformes para castigar, prevenir y penalizar el delito informático, son razones que justifican este tipo de investigaciones.

En el primer capítulo de este estudio se analiza el estado de la cuestión sobre el delito informático en el marco del derecho comparado, tomando referentes de países desarrollados y de menor desarrollo, como los países

[3] TORRES BERNAL, C.A. Metodología de la investigación: para administración, economía, humanidades y ciencias sociales. Pearson Educación, 2006. p.58

latinoamericanos. En el segundo capítulo, se analiza el delito informático dentro del marco jurídico colombiano. El tercer capítulo analiza propiamente uno de los delitos informáticos tipificados en el código penal colombiano, como transferencia no consentida de activos.

Después de presentar los tres capítulos en respuesta a los objetivos planteado, se realiza la discusión de resultados, para finalmente presentar las conclusiones y recomendaciones derivadas del desarrollo de esta investigación, relacionando las diferentes fuentes bibliográficas que soportan la investigación monográfica.

CAPITULO I. EL DELITO INFORMÁTICO EN EL MARCO DEL DERECHO COMPARADO

En este aparte, se presenta una contextualización sobre los antecedentes o estado del arte relacionado con investigaciones sobre el delito informático y la consideración desde los diferentes marcos jurídicos de algunos países desarrollados y latinoamericanos. Se analiza y contextualiza el delito informático y su tratamiento teórico a la luz de las nuevas tendencias de la globalización y una sociedad del conocimiento y la información.

A. Antecedentes o estado del arte

La literatura existente sobre investigaciones relacionadas con el ciberdelito, es prolífica. Sin embargo, se han seleccionado aquellas investigaciones de mayor actualidad, relevancia y pertinencia para los fines de este estudio.

El delito informático no sólo afecta Colombia sino a todos los países, puesto que en la medida del crecimiento de la sociedad de la información, el uso de las TIC, las redes sociales en todos los ámbitos económicos, sociales, políticos y culturales, obliga a los organismos internacionales y estados nacionales a realizar un frente común a través de la modificación de las leyes que protejan y castiguen la ciberdelincuencia, que ha traspasado fronteras y se vuelve cada vez más compleja en su identificación y aplicación de la normatividad en esta materia. Por lo tanto, a continuación se hace alusión a diferentes investigaciones en este

campo realizadas en otros contextos e investigaciones que permiten establecer referentes para abordar el estudio monográfico sobre el tema en cuestión.

Sobre referentes acerca del delito informático en el contexto internacional, está el estudio de ABU ISSA y otros[4]. Esta investigación se ocupa de aclarar las disposiciones legales del delito de acceso no autorizado a contenidos, según lo referido en el artículo 3 de la Ley de delito cibernético jordano de 2015 y lo compara con otras legislaciones árabes y la legislación francesa. En este estudio hace una aclaración sobre la posición de las convenciones internacionales acerca de este tipo de delitos. El análisis del delito de acceso no autorizado, incluye la definición de sus elementos, su sanción y las circunstancias agravantes para su penalización. Hace algunas recomendaciones para su inclusión por parte del legislador jordano, la actualización normativa y su adopción para prevenir y castigar el delito informático, en lo pertinente al acceso no autorizado a las redes de computadores.

Actualmente, junto con el avance de las TIC y el Internet, se habla sobre el Internet de las cosas (IoT, por sus siglas en inglés). Al respecto, está el estudio de YAQOOB y otros[5], sobre el Internet de las cosas forenses, los avances recientes,

[4] ABU ISSA, Hamzeh, ISMAIL, Mahmoud y AAMAR, Omar. Unauthorized access crime in Jordanian law (comparative study). [En_linea]: Digital Investigation. [2019/03/01/], 2019. vol. 28, p. 104-111

[5] YAQOOB, I., HASHEM, I. A. T., AHMED, A., KAZMI, S. M. A. y HONG, C. S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. [Traducción en linea] En: Future Generation Computer Systems. 2019. vol. 92, p. 265-275

taxonomía requisitos y desafíos abiertos. Los autores señalan que debido al crecimiento explosivo de los objetos inteligentes y su dependencia de las tecnologías inalámbricas para la comunicación, genera un aumento y vulnerabilidad del Internet de las cosas frente a los ataques cibernéticos. Por lo tanto, la investigación aporta diversas técnicas para rastrear dichos ataques internos y externos, enfatizando los mecanismos de comunicación y las vulnerabilidades arquitectónicas, lo cual es un avance para los gobiernos, las organizaciones empeñadas en combatir y castigar el delito cibernético y un referente para incorporar en las legislaciones de los países cooperantes y fomentar la investigación forense en este campo.

Otro referente internacional es el estudio de URBAN y otros[6], sobre la necesidad de aplicación de la ley en el campo de la lucha contra los delitos cometidos a través de Internet. Los autores señalan que debido a la amplia difusión de TICs, la naturaleza del delito está cambiando. En la actualidad, se cometen más y más delitos utilizando la tecnología informática e Internet. El propósito del estudio es el análisis de crímenes cometidos a través de Internet, proponiendo un sistema de medidas para combatir tales crímenes, aumentar la eficacia en la lucha contra los delitos informáticos, incluidas las relacionadas con el desarrollo de la cooperación internacional en el campo del derecho penal.

[6] URBAN, V.,KNIAZHEV, V.,MAYDYKOV, A.,YEMELYANOVA, E.. Implementation of the law enforcement function of the state in the field of countering crimes committed using the internet. Studies in Systems, Decision and Control. Springer International Publishing, 2019. Vol. 181, pgs. 113-120 [Traducción en línea]

Dentro de los referentes encontrados sobre el estado de la cuestión con respecto al delito informático, está el estudio de PROKOFIEVA y otros[7], sobre el Internet como zona delictiva: aspectos criminalistas y criminológicos. Los autores afirman que el rápido desarrollo de la red informática mundial de Internet a fines del siglo pasado, ha implicado un ataque inevitable por parte de organizaciones terroristas, asociaciones y grupos criminales, así como ciertos elementos criminales, en las infraestructuras de información y telecomunicaciones de los países industrializados. El estudio está dedicado a uno de los problemas reales de la sociedad moderna: Internet como zona delictiva. Como resultado de la investigación, se sugieren las principales medidas para contrarrestar la actividad terrorista en Internet, formas de combatir a los hackers-estafadores, así como otros delitos de Internet. Los datos obtenidos del estudio pueden usarse para predecir y contrarrestar los delitos cometidos en Internet.

Continuando con el análisis de los referentes sobre delitos informáticos, está el estudio de MAIMON y LOUDERBACK[8] acerca de los delitos ciberdependientes: una revisión interdisciplinaria. Los autores señalan que, el crimen en línea ha aumentado en severidad y frecuencia en las últimas dos décadas. Sin embargo, aunque varias disciplinas científicas han empleado

[7] PROKOFIEVA, E.,MAZUR, S.,CHERVONNYKH, E.,ZHURAVLEV, R. Internet as a crime zone: Criminalistic and criminological aspects.. [Traducción en línea] Springer International Publishing, 2019, Vol. 181 Pgs. 105-112

[8] MAIMON, D. y LOUDERBACK, E. R. Cyber-Dependent Crimes: An Interdisciplinary Review. [Traducción en línea] En: Annual Review of Criminology. 2019. vol. 2, p. 191-216

comúnmente teorías criminológicas para explicar este fenómeno, la criminología convencional ha dedicado una atención relativamente escasa a la investigación de los ciberdelincuentes y sus víctimas. Partiendo de esta suposición, se debe prestar más atención criminológica a este importante tipo de delito.

El artículo presenta una revisión interdisciplinaria del estado actual de la investigación sobre delitos ciberdependientes (es decir, delitos que requieren el uso de tecnología informática para existir, como la piratería). Comienzan con una breve discusión sobre el ecosistema de delitos ciberdependientes y los actores clave que operan dentro de él, incluidos los delincuentes y facilitadores en línea, objetivos y víctimas, y guardianes. Revisan la investigación empírica que pertenece a cada actor al tiempo que distinguen entre la investigación no teórica y los estudios teóricos. Luego detallan las vías metodológicas y teóricas que deberían ser buscadas por futuras investigaciones y discuten por qué la investigación criminológica debe liderar iniciativas de políticas y guiar el diseño de herramientas técnicas que mejoren la capacidad de la comunidad científica para generar un ciber-ambiente más seguro. Concluyen discutiendo las posibles formas en que la investigación del delito ciberdependiente podría allanar el camino para el avance de la teoría y la investigación criminológica convencional.

En este mismo contexto, se encontró el estudio de DONALDS y OSEI-BRYSON[9], denominado: Hacia una ontología de clasificación del delito cibernético, un enfoque basado en el conocimiento. Los autores comentan que, en los últimos años ha habido un aumento en los delitos cibernéticos y sus impactos negativos en la vida de las personas, organizaciones y gobiernos. Se ha argumentado que una mejor comprensión del delito cibernético es una condición necesaria para desarrollar respuestas legales y políticas adecuadas al delito cibernético. Si bien un esquema de clasificación universalmente acordado facilitaría el desarrollo de tal comprensión y también colaboraciones, los esquemas de clasificación actuales son insuficientes, fragmentados y a menudo incompatibles ya que cada uno se enfoca en diferentes perspectivas (por ejemplo, el papel de la computadora, el punto de vista del atacante o del defensor) o utiliza terminologías variables para referirse a la misma cosa, lo que hace improbables las clasificaciones consistentes de delitos informáticos. En este artículo presentan e ilustran una nueva ontología del delito cibernético que incorpora múltiples perspectivas y ofrece un punto de vista más holístico para la clasificación del delito cibernético. Por lo tanto, los hallazgos y propuesta deberían ser una herramienta más útil para el interés de los gobiernos empeñados en combatir el cibercrimen.

Otro estudio que permite contextualizar el cibercrimen internacional, corresponde al de Tosoni (2018), quien aborda el repensar de la privacidad en la

[9] DONALDS, C. y OSEI-BRYSON, K. M. Toward a cybercrime classification ontology: A knowledge-based approach. [Traducción en línea] En: Computers in Human Behavior. 2019. vol. 92, p. 403-418

Convención del Consejo de Europa sobre Cibercrimen. Este artículo examina la medida en que las consideraciones de privacidad de datos están integradas y equilibradas en los capítulos de derecho sustantivo, derecho procesal y cooperación internacional de la Convención sobre Cibercrimen del Consejo de Europa, a la luz de la redacción de un protocolo adicional a la Convención que se supone debe abordar, entre otros, los aspectos de privacidad de datos de las investigaciones de delitos cibernéticos, el artículo proporciona un análisis sobre las disposiciones de la Convención con sentido crítico con respecto a no proporcionar una privacidad adecuada de protección contra el ciberdelito. El argumento básico presentado en el artículo es que las preocupaciones sobre el potencial de la Convención para reducir la protección de la privacidad están en gran parte fuera de lugar. Sin embargo, el artículo destaca la necesidad de una mayor orientación prescriptiva sobre la privacidad de los datos para la aplicación de la ley.

Continuando con el análisis de referentes, está el artículo de RAHARJO y otros[10], el cual versa sobre: La influencia del determinismo tecnológico en la formación de actos penales en la legislación. Los autores plantean que, la tecnología ha entrado en la existencia física y espiritual humana. La tecnología es el reflejo del alma humana en la naturaleza, es la materialización de ideas en el cerebro humano mismo. Los humanos están cada vez más fragmentados y las

[10] RAHARJO, A.,SAEFUDIN, Y.,FIDIYANI, R. The influence of technology determinism in forming criminal act of legislation. EDP Sciences, Vol. 73 Pgs. 23-45 [Traducción en línea]

máquinas son cada vez más dominantes en la vida humana, lo que causa problemas en la tipificación de actos delictivos en diversas legislaciones. Para aclarar este problema, los métodos de investigación normativa se utilizan con un enfoque en la legislación comparativa. Las leyes de naturaleza cada vez más tecnológica adoptan características legales en el trabajo de la ciencia y la tecnología. Los legisladores hacen reglas que reflejan el determinismo tecnológico y también en contra, glorifican la tecnología y hacen de la tecnología uno de los factores de responsabilidad penal. Esto parece en la comparación entre la legislación de derecho penal general que se origina en el Código Penal con otras leyes y reglamentos que contienen elementos tecnológicos. Las sanciones penales basadas en la tecnología en el derecho penal general son desconocidas, y esto solo surge después de que la tecnología se utiliza para cometer actos criminales, como en actos criminales de decencia, humillación, difamación y tecnología de dimensión criminal. Esta razón debe ser descifrada considerando que los legisladores son pobres para dar una explicación.

Como complemento al estado de la cuestión sobre estudios e investigaciones relacionadas con el delito informático en diferentes contextos, se relaciona los principales artículos de actualidad que abordan esta temática, tales como el de FERREIRA[11] que realiza analiza la Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y

[11] FERREIRA, Eduardo. La Convención de Cibercrimen de Budapest y América Latina:Breve guía acerca de su impacto en los derechos y garantías de las personas. Área Digital de la Asociación por los Derechos Civiles (ADC) 2018), p. 1-14.

garantías de las personas; el artículo de CAI y otros[12], Du, Xin, & Chang (2018), donde analiza las características de los delitos cibernéticos: evidencia de documentos judiciales chinos; el estudio de BROWN y SMITH[13], donde hace una exploración sobre la relación entre crimen organizado y crimen de volumen: el artículo de BLYTHE y COVENTRY[14], que es un estudio comparativo de los factores que influyen en los comportamientos antimalware de los empleados; el artículo de BARRIOS A.[15], sobre Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015; el artículo de POSADA[16], sobre el cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual; el estudio de POLAŃSKI[17], que aborda el Ciberespacio: ¿una nueva rama del derecho internacional consuetudinario?;

[12] CAI, T., DU, L., XIN, Y. y CHANG, L. Y. C. Characteristics of cybercrimes: evidence from Chinese judgment documents. [Traducción en línea] En: Police Practice and Research. 2018. vol. 19, no. 6, p. 582-595

[13] BROWN, R. y SMITH, R. G. Exploring the relationship between organised crime and volume crime. [Traducción en línea] En: Trends and Issues in Crime and Criminal Justice. 2018, no. 565 Pg. 1-15

[14] BLYTHE, J. M. y COVENTRY, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. [Traducción en línea] En: Computers in Human Behavior. 2018. vol. 87, p. 87-97

[15] BARRIOS A., M. Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015. España: Editorial Reus S.A., 2018.

[16] POSADA M., Ricardo. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. En: Nuevo Foro Penal. 2017. vol. 13, no. 88, p. 72-112

[17] POLAŃSKI, Paul Przemysław. Cyberspace: A new branch of international customary law? En: Computer Law & Security Review. 2017/06/01/, 2017. vol. 33, no. 3, p. 371-381[Traducción en línea]

El artículo de NGO y JAISHANKAR[18], que analiza el Ciberespacio: ¿una nueva rama del derecho internacional consuetudinario?; el estudio de AZAD y otros[19], sobre áreas problemáticas de delitos cibernéticos, áreas legales y la ley de delitos cibernéticos; el artículo de VARGAS y otros[20], quien aprovechando el análisis de datos expone patrones de *phishing* contra una importante institución financiera de EE. UU. A su vez, SUÁREZ S[21]., hace un análisis sobre el Delito Informático en Colombia, análisis dogmático de Ley 1273 de 2009. Por su parte, ROJAS PARRA[22] realiza un análisis de la penalización del cibercrimen en países de habla hispana; HILL y MARION[23] hace una introducción al delito cibernético: delitos informáticos, leyes y vigilancia en el siglo XXI; GERRY QC y otros[24], analiza el papel de la tecnología en la lucha contra la trata de personas: reflexiones sobre la

[18] NGO, F. y JAISHANKAR, K. Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cybercrime. [Traducción en línea] En: International Journal of Cyber Criminology. 2017. vol. 11, no. 1, p. 1-9

[19] AZAD, D, NAFIUL MAZID, Kazi y SHARMIN, Syeda. Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law. [Traducción en línea] En: International Journal of New Technology and Research. 05/01, 2017. vol. 3, p. 1-6

[20] VARGAS, J.,BAHNSEN, A. C.,VILLEGAS, S.,INGEVALDSON, D. Knowing your enemies: Leveraging data analysis to expose phishing patterns against a major US financial institution. eCrime Researchers Summit, eCrime. Vol. 2016-June, pg. 52-61 [Traducción en línea]

[21] SUÁREZ S., A. Manual de Delito Informático en Colombia. Análisis dogmático de Ley 1273 de 2009. Bogotá: Universidad Externado de Colombia, 2016.

[22] ROJAS PARRA, Jaime Hernán. Análisis de la penalización del cibercrimen en países de habla hispana. En: Revista Logos, Ciencia & Tecnología. 2016. vol. 8, no. 1, p. 220-231

[23] HILL, J.B. y MARION, N.E. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st. ABC-CLIO, 2016

[24] GERRY QC, Felicity, MURASZKIEWICZ, Julia y VAVOULA, Niovi. The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. [Traducción en línea] En: Computer Law & Security Review. 2016/04/01/, 2016. vol. 32, no. 2, p. 205-217

privacidad y la protección de datos; BARN y BARN[25] hace una representación ontológica de una taxonomía para el cibercrimen. SUÁREZ S[26]., analiza la Estafa Informática; SMITH[27], plantea modelos de gestión del cibercrimen internacional y, finalmente SOBRINO HEREDIA y SÁNCHEZ GÓMEZ[28] plantea retos del derecho ante las nuevas amenazas.

B. Contexto del delito informático

El delito cibernético o delito informático, es un delito que involucra una computadora y una red. La computadora puede haber sido utilizada en la comisión de un delito, o puede ser el objetivo. Los delitos cibernéticos se definen como: Delitos cometidos contra individuos o grupos de individuos con un motivo criminal para dañar intencionalmente la reputación de la víctima o causar daño físico o mental, o pérdida patrimonial, a la víctima directa o indirectamente, utilizando redes de telecomunicaciones modernas como Internet (redes que incluyen, entre otras, salas de chat, correos electrónicos, tablones de anuncios y grupos) y teléfonos móviles (Bluetooth/SMS/MMS). El delito cibernético puede amenazar la seguridad

[25] BARN, R., BARN, B. An ontological representation of a taxonomy for cybercrime. Association for Information Systems, 2016 p. 12-15

[26] SUÁREZ S., A. La Estafa Informática. Bogotá: Grupo Editorial Ibañez, 2015, p.195

[27] SMITH, G. S. Management models for international cybercrime. [Traducción en línea] En: Journal of Financial Crime. 2015. vol. 22, no. 1, p. 104-125

[28] SOBRINO HEREDIA, José Manuel y SÁNCHEZ GÓMEZ, Fernando J. Retos del derecho ante las nuevas amenazas. Madrid, ES: Dykinson, 2014. p. 400

financiera de una persona o de una nación. Los problemas relacionados con este tipo de delitos se han vuelto de alto perfil, particularmente aquellos relacionados con la piratería, infracción de derechos de autor, vigilancia masiva injustificada y pornografía infantil. También hay problemas de privacidad cuando la información confidencial es interceptada o revelada, ilegalmente o de otra manera[29].

El delito informático es ejecutado por un usuario informático conocedor, a veces denominado pirata informático que navega o roba ilegalmente información privada de una empresa o personas. En algunos casos, esta persona o grupo de individuos puede ser maliciosos y destruir o dañar la computadora o los archivos de datos. Alternativamente se conoce como delito cibernético, delito electrónico, delito electrónico o delito de alta tecnología. También, la actividad ilícita que cruza fronteras internacionales y que involucra los intereses de al menos un Estado-nación a veces se denomina guerra cibernética[30].

El delito informático dadas sus características especiales que configuran el hecho punible y las variables, elementos y medios que hacen visible la ejecución del acto, es definido de forma genérica por la Real Academia de la Lengua Española como la “infracción penal cometida utilizando un medio o instrumento informático”.

[29] AZAD, D, NAFIUL MAZID, Kazi y SHARMIN, Syeda. Op. Cit.

[30] DONALDS, C. y OSEI-BRYSON, K. M. Op.Cit.

Por su parte FERNÁNDEZ CALVO[31] citando al Profesor *Miguel Ángel Davara*, define el delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos".

En ese mismo sentido MARIA DE LA LUZ LIMA[32] aborda el delito informático asociado al medio electrónico, con base a la configuración del comportamiento criminal visibilizando algunas de sus características, indicando que:

> El delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin y que, en su sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.
>
> Como método: Son conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
>
> Como medio: Son conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.

[31] FERNÁNDEZ CALVO. Rafael. El tratamiento del llamado delito informático en el Proyecto de Ley Orgánica del Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática). En: Informática y Derecho. p.1150

[32] LIMA DE LA LUZ. Maria. Delitos electrónicos. En: Criminalia. Academia Mexicana de Ciencias Penales. Edit. Porrúa, No. 1-6, 1984. p. 100

> Como fin: Son conductas criminales dirigidas contra la entidad física del objeto o maquina electrónica o su material con objeto de dañarla.

Otro estudioso del tema y especialista en derecho informático y derecho de las nuevas tecnologías como es el caso del Profesor TÉLLEZ VALDÉS[33] ha definido el delito informático y sus características, precisando que:

> Los delitos informáticos son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).

Frente a las características del delito informático señala:

1. Son conductas delictivas de cuello blanco[34] (*White collar crimes),* en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

[33] TÉLLEZ VALDÉS. Julio. Derecho informático 3ª Edición. McGraw-Hill Interamericana Editores S.A. DE C.V. México. 2004. p. 163

[34] *Delitos de cuello blanco, "*termino introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en el año 1943, refiriéndose a aquellas conductas que pueden no estar tipificadas en algunos ordenamientos jurídicos como delitos, destacando violaciones a las leyes de patentes y derechos de autor, mercado negro, contrabando en empresas, evasión de impuestos, quiebras fraudulentas y corrupción de altos funcionarios", entre otros. Para TÉLLEZ VALDÉS estos delitos "son los cometidos por gente con alto estatus socioeconómico y con preparación técnica o profesional en alguna ciencia" (Tomado de TÉLLEZ VALDÉS. Julio. Derecho informático 3ª Edición. McGraw-Hill Interamericana Editores S.A. DE C.V. México. 2004. p. 164

2. Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto está en el trabajo.
3. Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.
6. Son muchos los casos y pocas las denuncias, todo ello debido a la falta misma de regulación jurídica a nivel internacional.
7. Son sumamente sofisticados y frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).
10. Ofrecen facilidades para su comisión a los menores de edad.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica a nivel internacional.

Las principales áreas críticas de alto riesgo que se originan por los delitos cibernéticos están asociados con las telecomunicaciones, el vandalismo electrónico, terrorismo y extorsión, el hurto de servicios de telecomunicaciones, la piratería en telecomunicaciones, la pornografía y divulgación de material ofensivo,

así como el fraude en procesos de tele mercadeo; por último, el delito asociado a la experiencia electrónica de fondos, que para el caso colombiano, se traduce en la transferencia no consentida de activos[35].

C. Desafíos y preguntas de investigación sobre delito informático

La proliferación de delitos informáticos conlleva realizar muchos interrogantes para la legislación de los países sobre la aplicación de la ley relacionada con la búsqueda de incautación de pruebas electrónicas como vestigio de la comisión de delitos informáticos en Internet y en otros dispositivos electrónicos inherentes a TICs. Al respecto, varios estudios BLYTHE y COVENTRY[36], BROWN y SMITH[37], 2018; CAI y Otros[38]; NGO y JAISHANKAR, PAUL JOSEPH y NORMAN[39] y analistas sobre criminología plantean varios interrogantes, que la ley y las jurisdicciones de los países deben dar respuesta para combatir el ciberdelito en todas sus modalidades. A continuación, se relacionan los principales interrogantes, como un referente para la reflexión, el análisis y la investigación en el contexto del delito informático. Según MAIMON y LOUDERBACK[40], los problemas en materia

[35] PROKOFIEVA, E.,MAZUR, S.,CHERVONNYKH, E.,ZHURAVLEV, R.Op. Cit.

[36] Op. Cit.

[37] Op. Cit.

[38] Op. Cit

[39] PAUL JOSEPH, D.,NORMAN, J. An analysis of digital forensics in cyber security. Springer Verlag, 2019, Vol 815, pp. 701-708 [Traducción en línea]

[40] Op. Cit.p., 205

de investigación desde el ámbito de la aplicación de la ley y la actualización jurídica para los países, puede resumirse en dar respuesta a los siguientes interrogantes:

(i) ¿Distingue la ley entre la búsqueda y la incautación de datos almacenados en una computadora y la interceptación de datos que se comunican de una computadora a otra o dentro de un sistema informático?

(ii) ¿Puede una persona proporcionar voluntariamente a los agentes de la ley datos electrónicos que puedan generar evidencia de un delito? ¿Puede una persona permitir voluntariamente a los agentes del orden realizar una búsqueda de dichos datos, en lugar de proporcionarlos? ¿Podría una cooperación continua de esta naturaleza por parte de una persona con aplicación de la ley tener un efecto legal sobre la capacidad de la aplicación de la ley para obtener o usar los datos?

(iii) En la mayoría de las jurisdicciones, la capacidad de las fuerzas del orden público para obtener datos que puedan proporcionar evidencia generalmente requiere alguna forma de aprobación judicial previa. ¿Qué autoridad legal se requiere para obtener datos electrónicos almacenados, sin el consentimiento de las personas interesadas?

(iv) Los datos electrónicos en la mayoría de las jurisdicciones se consideran intangibles. La ley de algunas jurisdicciones solo puede permitir la incautación de material tangible. En tales casos, los datos intangibles solo se pueden obtener incautando el medio físico (por ejemplo, datos en disquete u otro medio de almacenamiento) en el que se almacenan y se encuentran los datos. ¿Las leyes de su país

prevén la incautación de datos intangibles sin la incautación del medio físico que se encuentra?

(v) En algunos casos, la ubicación precisa de los datos electrónicos dentro de un sistema informático puede no ser evidente. ¿Qué tan específica debe ser la descripción en la autoridad judicial (p. Ej., Orden de allanamiento) para buscar los datos a confiscar?

(vi) En la mayoría de las jurisdicciones, el alcance de una orden debe ser lo más limitado posible. La ubicación precisa de los datos electrónicos puede no ser inmediatamente aparente en el momento en que se solicita una orden judicial, o incluso cuando los agentes de la ley llegan al lugar. ¿Proporciona la ley orientación sobre si aprovechar todo el sistema informático o solo uno o más de sus componentes? ¿Qué criterios prácticos utilizan las fuerzas del orden para tomar esta decisión? ¿Cómo se haría esto en la práctica?

(vii) ¿Su ley obliga a un sospechoso o una tercera persona a proporcionar acceso (incluidas las contraseñas) a un sistema informático que es objeto de una búsqueda legal? De no ser así, ¿qué medidas prácticas o herramientas pueden emplear las fuerzas del orden para obtener acceso?

(viii) La incautación durante el curso de una búsqueda que da lugar al cierre de un sistema informático completo puede ser extremadamente intrusivo y particularmente oneroso para un negocio en curso. ¿Qué circunstancias prácticas justificarían incautar o cerrar un sistema completo en lugar de simplemente tomar una copia de los datos? ¿La ley prevé la copia de datos relevantes como una alternativa a la incautación, y puede la copia ser considerada como evidencia admisible? ¿Permitiría la ley la incautación de toda la base de datos con el fin de identificar posteriormente los datos relevantes?

¿Qué medios prácticos se pueden utilizar para copiar grandes volúmenes de datos?

(ix) En el curso de una búsqueda, las autoridades policiales pueden encontrar datos incriminatorios relacionados con el delito investigado, pero que no se especificaron originalmente dentro del alcance de la orden. ¿Se pueden confiscar legalmente estos datos sin obtener otra orden?

(x) En el curso de una búsqueda, las autoridades encargadas de hacer cumplir la ley pueden encontrar datos electrónicos relacionados con un delito diferente del que se encuentra bajo la investigación actual. ¿Se pueden confiscar legalmente estos datos sin obtener otra orden?

(xi) ¿La ley permite la incautación de datos sin una orden judicial en circunstancias exigentes, como cuando existe el riesgo de borrado o destrucción de datos? Alternativamente, ¿pueden los agentes de la ley asegurar las instalaciones o el sistema informático, en espera de la obtención de una orden judicial?

(xii) En algunos casos, los datos buscados pueden estar ubicados en otro sistema informático que esté conectado en red al sistema que se está buscando actualmente. ¿La ley permite una extensión de la búsqueda en el sistema conectado para buscar y confiscar datos relevantes dentro del alcance de la orden? ¿La orden puede incluir una autorización para extender la búsqueda al sistema conectado? Alternativamente, ¿puede la policía obtener una segunda orden para extender la búsqueda de un sistema a otro?

(xiii) ¿Hay alguna circunstancia bajo la cual la ley permita que los datos almacenados se obtengan mediante una orden judicial para

entregar dichos datos a las autoridades policiales, en contraposición a las propias autoridades policiales que los buscan y confiscan?

Las anteriores interrogantes, suponen un escenario para la reflexión por cuanto es un desafío permanente para los países y sus legislaciones en el marco del Convenio de Budapest, que en una de sus consideraciones del preámbulo señala que los países signatarios están "Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional"[41]

D. Derecho cibernético y tecnología de la información

El éxito en cualquier campo de la actividad humana lleva al crimen, que necesita mecanismos para controlarlo. Las disposiciones legales deben proporcionar seguridad a los usuarios, empoderamiento a las agencias de aplicación de la ley y disuasión a los delincuentes. La ley es tan estricta como su aplicación. El crimen ya no se limita al espacio, el tiempo o un grupo de personas. El ciberespacio crea errores morales, civiles y criminales. Ahora ha dado una nueva forma de expresar tendencias criminales, "en 1990, menos de 100,000 personas pudieron iniciar

[41] Convenio de Budapest, 2001, p.1

sesión en Internet en todo el mundo. Ahora, alrededor de 500 millones de personas están conectadas a navegar por la red en todo el mundo”[42]

Hasta hace poco, muchos profesionales de la tecnología de la información (TI) carecían de conciencia e interés en el fenómeno del delito cibernético. En muchos casos, los funcionarios encargados de hacer cumplir la ley carecen de las herramientas necesarias para abordar el problema; las viejas leyes no encajaban con los crímenes cometidos, las nuevas leyes no habían captado la realidad de lo que estaba sucediendo, y había pocos precedentes judiciales para buscar orientación. Además, los debates sobre cuestiones de privacidad obstaculizaron la capacidad de los agentes encargados de hacer cumplir la ley para reunir la evidencia necesaria para procesar estos nuevos casos. Finalmente, hubo una cierta cantidad de antipatía, o al menos desconfianza, entre los dos actores más importantes en cualquier lucha efectiva contra el cibercrimen: las agencias de aplicación de la ley y los profesionales de la informática. Sin embargo, una estrecha cooperación entre los dos es crucial si queremos controlar el problema del delito cibernético y hacer de Internet un "lugar" seguro para sus usuarios[43].

Junto con el crecimiento masificado de Internet, el intercambio y almacenamiento de información de manera rápida y económica, ha tenido

[42] TWENEBOAH-KODUA, S., ATSU, F. y BUCHANAN, W. Impact of cyberattacks on stock performance: a comparative study. En: Information and Computer Security. 2018. vol. 26, no. 5, p. 640. [Traducción en línea]

[43] KUMAR, A.P. Cyber Law. Mr.Anupa Kumar Patri, 2009 p.109

incidencia en la actividad delictiva cibernética, desde la infracción de derechos de autor hasta el *phishing* y la pornografía en línea, también se ha incrementado. Estos crímenes, tanto antiguos como nuevos, plantean desafíos tanto para las autoridades como para los legisladores. ¿Qué esfuerzos, si los hay, podrían disuadir el delito cibernético en el mundo moderno altamente interconectado y extremadamente rápido? Comprender el delito cibernético: delitos informáticos, leyes y vigilancia policial en el siglo XXI, "es un desafió permanente para los gobiernos en torno a abordar esta difícil cuestión para lo cual es necesario contextualizar mejor el lugar que ocupa la comisión del delito cibernético en el panorama actual del mundo global y la incidencia en la sociedad actual"[44].

E. Naturaleza transnacional del delito cibernético

A un nivel puramente técnico, todos los mensajes en Internet se dividen en paquetes que se separan y viajan a través de enrutadores y servidores disponibles ubicados en todo el mundo. El delito cibernético va más allá de esta dimensión técnica y transnacional e involucra a remitentes que deliberadamente diseñan sus ataques y otros delitos para explotar las debilidades potenciales presentes en la naturaleza transnacional de la infraestructura tecnológica de los países. Estas debilidades incluyen: (1) un grupo objetivo mundial de computadoras y usuarios para victimizar o explotar en ataques de denegación de servicio u otros, lo que

[44] HILL, J.B. y MARION, N.E. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st. ABC-CLIO, 2016, p.290 [Traducción en línea]

permite a los atacantes hacer más daño sin más esfuerzo del necesario para atacar computadoras o usuarios en un solo Estado; y (2) las disparidades generalizadas entre los Estados, en el entorno legal, regulatorio o de políticas relacionadas con el delito cibernético, y la falta de un grado suficientemente alto de cooperación internacional para procesar y disuadir dicho delito. Los ciberataques más dañinos experimentados hasta ahora han sido transnacionales, originados en muchos países diferentes y dirigidos a computadoras en todas partes del mundo[45].

F. La mala imagen del Internet y las TIC

Con respecto a los avances impresionantes de Internet y las tecnologías de la información y las comunicaciones (TIC), su manifestación popular a través de los medios de comunicación de periódicos, revistas, transmisiones de radio y televisión, a menudo se ha centrado en la especulación sobre los efectos perjudiciales de las TIC en varios aspectos de la aplicación de la ley, la seguridad y el orden social. Internet, por ejemplo, se representa con frecuencia como una especie de dominio virtual oscuro habitado por una mezcla de piratas informáticos disidentes, delincuentes organizados, grupos políticos extremistas y proveedores de imágenes pornográficas. En consecuencia, las TIC interactivas se consideran un medio para facilitar las actividades delictivas antisociales que socavan la seguridad nacional y la aplicación de la ley y, por lo tanto, amenazan el tejido

[45] GOODMAN, S.E. y SOFAER, A.D. The Transnational Dimension of Cyber Crime and Terrorism. Hoover Institution Press, 2013. p. 292 [Traducción en línea]

social de las sociedades capitalistas democráticas. No es de extrañar entonces ser testigos de la alarma pública sobre los nuevos medios como consecuencia de este sensacional reportaje[46].

Pero, ¿estas selecciones altamente publicitadas y sensacionales del uso de las TIC para emprendimientos criminales nos brindan una imagen precisa de la amenaza percibida para nuestro orden social y económico? ¿Cuál es el alcance del delito grave en Internet? ¿No hay peligro de que esta publicidad pueda contribuir a un "pánico moral" y una reacción contra la libre expresión? Además, ¿cuáles son las garantías para la privacidad y el anonimato frente a las demandas de tales tecnologías para su vigilancia y detección? [47].

Los desafíos a los que se enfrentan los sistemas legales, las infraestructuras nacionales críticas y las agencias de seguridad como consecuencia del uso de las nuevas TIC por parte de los activistas criminales son ciertamente trascendentales. Sin embargo, la validez y la efectividad de las acciones y políticas adoptadas para abordarlas requieren una deliberación más considerada que la que actualmente se encuentra en el verbo histérico que emana de la mayoría de los medios populares[48].

[46] BARN, R., BARN, B. Op. Cit.

[47] BLYTHE, J. M. y COVENTRY, L.Op. Cit.

[48] LOADER, B.D. y THOMAS, D. Cybercrime: Security and Surveillance in the Information Age. Taylor & Francis, 2013, p.390 [Traducción en línea]

G. Sobre el cibercrimen

Los delitos cibernéticos son delitos penales relativamente nuevos y son el resultado de los recientes avances en tecnología informática e Internet. Hoy, Internet es una parte esencial de la vida cotidiana para la mayoría de las personas. La mayoría de las empresas, los gobiernos y los individuos confían en esta nueva tecnología como parte de su rutina diaria. Las computadoras se usan en hogares, negocios, consultorios médicos, bibliotecas y escuelas. Han cambiado la forma en que las personas trabajan, se comunican y socializan en su vida diaria. Muchas personas usan Internet todos los días para realizar negocios, realizar investigaciones, recopilar información, comprar, entretener, pagar bienes y servicios, realizar tareas bancarias y financieras, enviar archivos y datos a otros y comunicarse con amigos y familiares de todo el mundo. "De hecho, se estima que alrededor del 61% de la población de la Tierra usa Internet regularmente"[49].

Muchos de los cambios resultantes de la tecnología han beneficiado claramente a la sociedad. Se ha visto avances en medicina, ciencias sociales e ingenierías. También se ha mejorado la comunicación entre empresas, clientes y empleados. Los documentos están disponibles más fácilmente y son más seguros. Muchas empresas se han "vuelto verdes" como una forma de proteger el medio ambiente. Incluso se ha visto cambios en el lugar de trabajo para que los

[49] PROKOFIEVA, E.,MAZUR, S.,CHERVONNYKH, E.,ZHURAVLEV, R.Op. Cit. p.108

empleados ya no se vean obligados a trabajar en una oficina durante ocho horas seguidas. En cambio, pueden trabajar desde casa u otro lugar en cualquier momento del día o de la noche[50].

Si bien los avances tecnológicos han beneficiado a la sociedad, también han creado nuevas oportunidades para los ciberdelincuentes que utilizan estas innovaciones para causar daño a otros. A medida que la tecnología se ha desarrollado, también lo han hecho los nuevos delitos que dependen de esa tecnología. Muchos de estos delitos, como la piratería informática o la introducción de spyware, no existirían si no fuera por la tecnología informática. Y a medida que la tecnología informática se vuelve más avanzada, también lo hacen las actividades ilegales. Constantemente se desarrollan nuevos delitos en el ámbito del ciberespacio, convirtiéndose en un desafío permanente para las legislaciones de los países, dado que el ciberdelito cruza fronteras y en la mayoría de los casos la jurisdicción para la aplicación de la ley se vuelve compleja y difícil de comprobar[51].

No solo han surgido nuevos crímenes, sino que también se han transformado algunos crímenes más tradicionales para la sociedad del conocimiento y la información. Los delitos tradicionales como el fraude, la

[50] HILL, J.B. y MARION, N.E.Op. Cit.

[51] Singh, S. K., Rastogi, N. Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study. Institute of Electrical and Electronics Engineers Inc. 2018 p. 18-23 [Traducción en línea]

apropiación ilícita, el acoso escolar, que han sido parte de nuestra sociedad durante años, ahora ocurren pero bajo nuevas formas o maneras de manifestación y afectación a las víctimas. Las drogas ilegales y la pornografía infantil, que existían antes del desarrollo de la tecnología de red, ahora se venden a través de Internet. Las transacciones financieras (por ejemplo, mal uso de tarjetas de crédito) y los delitos de lavado de dinero se han convertido en nuevas formas de delincuencia. En algunos casos, Internet ha hecho que la comisión de estos crímenes sea mucho más simple y de mayor frecuencia por las oportunidades que se ofrece a la delincuencia[52].

Estos nuevos delitos están ocurriendo porque son relativamente fáciles de cometer. Los ciberdelincuentes pueden piratear fácilmente los sistemas informáticos en cualquier parte del mundo con poco costo y poco riesgo de ser atrapados. Pueden alterar registros e información, apropiarse dinero o de la identidad de víctimas inocentes. Pueden ofrecer bienes y productos en venta que no se pueden comprar en otro lugar. Los mensajes se pueden publicar con la intención de dañar la reputación de una persona. El software necesario para llevar a cabo todos estos ataques maliciosos se puede comprar en línea por una pequeña tarifa[53].

[52] AZAD, Dr, NAFIUL MAZID, Kazi y SHARMIN, Syeda.Op. Cit.

[53] REEP-VAN DEN BERGH, C. M. M. y JUNGER, M. Victims of cybercrime in Europe: a review of victim surveys. [Traducción en línea] En: Crime Science. 2018. vol. 7, no. 1, p. 1-7

Debido a la facilidad con que se pueden cometer estos delitos, las estadísticas muestran un constante crecimiento. Pero a la par, también pueden ser delitos de mayor peligrosidad y afectación a las personas. Así por ejemplo, en 2016, el Foro Económico Mundial afirmó que el delito cibernético es uno de los mayores riesgos para la estabilidad financiera y política mundial. Si tienen éxito, los delincuentes cibernéticos tienen el potencial de paralizar la economía mundial[54].

Cibercrimen

"Cibercrimen" es un término muy amplio que a menudo se usa para referirse a diferentes conceptos. En consecuencia, existe cierto debate sobre el significado exacto del término. El delito cibernético puede considerarse como un delito que involucra computadoras y redes de computacionales. En general, el cibercrimen se refiere a actos que involucran la tecnología para fines criminales y afectar a las personas, las organizaciones y los Estados, mediando el uso de Internet u otros sistemas en red para causar daño o alguna forma de perturbación cibernética. Puede incluir cualquier actividad delictiva, no solo en computadoras, redes o Internet, sino también en teléfonos móviles u otros dispositivos personales, que tiene la intención de causar daño a otros. El cibercrimen está asociado con actividades ilegales que se realizan a través de redes electrónicas globales. En resumen, el término cibercrimen se refiere a los métodos por los cuales las

[54] HILL, J.B. y MARION, N.E.Op.Cit.

computadoras u otros dispositivos electrónicos se utilizan para llevar a cabo actividades delictivas y causar daño a terceros [55].

Un delito cibernético podría ser el uso indebido de sistemas o redes informáticas para llevar a cabo delitos punibles mediante el acceso no autorizado a un sistema informático, la intercepción ilegal o la alteración de datos, o el uso indebido de dispositivos electrónicos. Dentro del alcance del delito cibernético puede estar el hurto de propiedad intelectual, es decir, la apropiación de una patente, secreto comercial o cualquier cosa protegida por las leyes de derechos de autor. También puede incluir ataques contra computadoras para interrumpir deliberadamente el procesamiento o actos de espionaje para hacer copias no autorizadas de datos clasificados[56].

El delito cibernético también incluye descargar música ilegal, hurto de dinero de cuentas bancarias, crear virus, publicar información comercial confidencial en Internet, comprometer la identidad de una persona mediante la suplantación de identidad o fraude, tráfico de pornografía infantil, lavado de dinero y falsificación, y cometer ataques de denegación de servicios informáticos. Otros ejemplos de delitos cibernéticos incluyen virus informáticos; malware correos electrónicos o sitios web falsos; la suplantación de identidad; acoso cibernético, acoso u

[55] Ibid. p. 25

[56] FERREIRA, Eduardo. La Convención de Cibercrimen de Budapest y América Latina:Breve guía acerca de su impacto en los derechos y garantías de las personas. Área Digital de la Asociación por los Derechos Civiles (ADC) 2018), p. 1-14

hostigamiento; estafas en línea; apropiación ilícita de una tarjeta de crédito; o *phishing*, entre otros[57].

El término delito cibernético a menudo abarca otras categorías más específicas de comportamiento ilegal, es decir, los delitos asistidos por computadora y los delitos centrados en la computadora. El término de delito informático a veces se refiere a los mismos actos delictivos informáticos, digitales o tecnológicos. Todos estos términos se refieren a actividades delictivas que se cometen mediante el uso de tecnologías digitales, de red o informáticas emergentes, como Internet[58].

En la Unión Europea, el Consejo de Europa proporciona una definición más completa de cibercrimen. Describe el delito cibernético como aplicado a tres categorías de actividades delictivas. El primero, cubre las formas tradicionales de delincuencia, como el fraude o la falsificación, aunque en un contexto de delito cibernético se relaciona específicamente con delitos cometidos a través de redes de comunicación electrónica y sistemas de información. El segundo, se refiere a la publicación de contenido ilegal en medios electrónicos (es decir, material de abuso sexual infantil o incitación al odio racial). El tercero, incluye crímenes exclusivos de las redes electrónicas, es decir, ataques contra sistemas de información, negación de envío y piratería. Estos tipos de ataques también pueden dirigirse contra

[57] RAHARJO, A.,SAEFUDIN, Y.,FIDIYANI, R.Op. Cit.

[58] HILL, J.B. y MARION, N.E.Op. Cit.

infraestructuras críticas cruciales y afectan los sistemas de alerta rápida existentes en muchas áreas, con un potencial desastroso y con consecuencias para toda la sociedad. Es común que cada categoría de delito se cometa a gran escala y con una gran distancia geográfica entre el acto criminal y sus efectos.

En consecuencia, los aspectos técnicos de los métodos de investigación aplicados son a menudo los mismos en todos los tipos de ataque[59].

El cibercrimen desde la mirada de un experto

La progresiva evolución de las Tecnologías de la Información y la Comunicación durante los últimos 20 años ha sido intensa, lo cual ha supuesto que los cambios sociales previstos hayan sido en muchos casos impredecibles y abruptos. En el caso de la cibercriminalidad de forma vertiginosa han surgido nuevos intereses sociales y nuevas formas de comisión de delitos tradicionales, frente a lo cual en muy poco tiempo han tenido que reinterpretarse las normas sustantivas y procesales, así como crearse otras nuevas. Los tratadistas del derecho se han visto obligados a abordar el tema en busca de soluciones jurídicas válidas para esas nuevas necesidades, afrontando en muchas ocasiones la dificultad de acometer esa tarea con el suficiente sosiego y la idónea perspectiva.

En este sentido, se destacan los aportes de MIRO LL., Fernando[60], quien en su obra, el cibercrimen tiene una dedicación muy característica que refleja las

[59] HILL, J.B. y MARION, N.E.Op. Cit. p. 26

bondades y riesgos de la tecnología en la actualidad donde las interacciones cada vez más se ausentan del espacio físico y se abren paso a otros medios asociados al ciberespacio. El cibercrimen opera en este nuevo escenario, requiriendo una clasificación integral de la cibercriminalidad que anticipe posibles afectaciones a quienes hacen uso de los sistemas informáticos. Las Tecnologías de la Información y la Comunicación (TIC), han venido generando cambios en la manera de comunicarnos, siendo el Internet el medio más representativo en la iteración continua en un mundo globalizado en el que el fortalecimiento de las relaciones interpersonales y la economía inciden ineludiblemente en la mutación del crimen, vislumbrando nuevas formas de comisión del mismo y afectando en mayor medida la sociedad. La continua evolución del ciberdelito permite entender

[60] Femando Miró Llinares es profesor de Derecho Penal y Criminología en la Universidad Miguel Hernández de Elche (España), Decano de la Facultad de Ciencias Sociales y Jurídicas de la misma Universidad y Presidente del Centro de Investigación CRIMINA para el estudio y la prevención del delito. Sus principales intereses de investigación se pueden dividir en dos áreas, (l) Derecho Penal, con respecto a la protección penal de los derechos de propiedad intelectual; la ley penal de seguridad vial y específicamente los delitos de negativa a someterse a pruebas de alcohol y conducir sin un permiso; participación criminal, en general, pero en base a ella también cuestiones claves como la imputación objetiva y el fraude, en general, y en el derecho penal corporativo en particular; y (2) Criminología, circunscrita al Cibercrimen, se basan en enfoques de Criminología Ambiental como la cibervictimización, actividades rutinarias, ciberplaces, radicalización en línea y el uso de tecnologías de Internet, entre otros, tanto desde un punto de vista teórico como empírico. Es uno de los especialistas en cibercrimen más reconocidos y citados en España, desarrollando contribuciones relevantes sobre la arquitectura del ciberespacio, las diferentes formas de victimización cibernética y el impacto del discurso de odio en línea.

El profesor Miró-Llinares forma parte de siete prestigiosas redes internacionales como la Sociedad Europea de Criminología (ESC), la Sociedad Estadounidense de Criminología (ASC), la Sociedad Española de Investigación Criminológica (SEIC), la Sociedad Internacional de Criminología (ISC), La Sociedad Internacional de Derecho Penal (ICLS), la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) y participa en los Simposios de Criminología Ambiental y Análisis de Delitos (ECCA).

Como investigador principal, ha liderado proyectos nacionales y regionales y ha participado en proyectos europeos como socio líder en factores humanos. Durante su carrera investigadora ha escrito 10 libros, más de 40 capítulos de libros y 40 artículos en varias revistas científicas y ha dado más de 100 conferencias en congresos, seminarios y simposios, entre otros.

mejor los aspectos fenomenológicos del acto criminal caracterizando el victimario «hacker» no solo como un sujeto que genera el ilícito a título individual, sino también como miembro de una estructura criminal organizada capaz de generar daño a gran escala, mientras que las victimas por su parte han implementado estrategias para prevenir y minimizar los efectos del delito[61].

El autor, uno de los principales tratadistas en derecho penal en el campo del ciberdelito a nivel de España, en su obra analiza la fenomenología del cibercrimen, abordando la criminalidad en el ciberespacio: la cibercriminalidad y tipos de cibercrimen y la clasificación de los mismos. En la segunda medida, estudia la criminología del cibercrimen, desarrollándola en tres apartados: ciberespacio y oportunidad delictiva; el cibercriminal. Perfiles de delincuentes en el ciberespacio y la cibervictima: perfiles de victimización y riesgo real de la amenaza de cibercrimen[62].

Sobre el cibercrimen, MIRO LL., Fernando genera una profunda reflexión frente a la necesidad de proscribir la expresión “delitos informáticos” por los vocablos cibercrimen y cibercriminalidad, los cuales describe asignándoles una definición de acuerdo a la función dialéctica que cumplen y las características que los rodean común y legalmente. El autor sustenta su posición frente al tema anotando que el peligro o inseguridad no depende en estricto sentido del uso de

[61] MIRO LL., Fernando. EL CIBERCRIMEN: Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012.

[62] Ibid. p. 18

tecnologías informáticas y/o de la información contenida en las mismas, sino que el riesgo subsiste en el “sistema de redes telemáticas intercomunicadas” y en la interacciones reciproca que se pueda generar en estas.

En su obra Fenomenología de la delincuencia en el ciberespacio, MIRO LL., Fernando adelanta una categorización de conductas delictivas asociadas al ciberespacio con el fin de entender en un sentido amplio la fenomenología criminal, a partir de la codificación de dos variables que inciden en el denominado cibercrimen. Por una parte, hace referencia a aquellas prácticas en las que las TIC tienen un papel preponderante en la comisión del ilícito considerando aspectos de invasión y afectación a través de sistemas informáticos que describe como, (i) “ciberataques puros” aludiendo a aquellos que solo ocurren en el ciberespacio y que son el resultado del desarrollo de las TIC; (ii) ciberataques réplica” que acoge los delitos en los que el ciberespacio es el medio a través del cual se cometen delitos tradicionales, dado que el ataque no se encuentra direccionado a un terminal informático, sino que la red es el entorno a través del cual se consuma el delito que en otro tiempo se generaba por diversos medios físicos, (iii) “ciberataques de contenido” que se relacionan con un perfil específico de los ataque réplica, pero con particularidades jurídicas que ameritan un tratamiento autónomo, teniendo en cuenta que agrupan aquellos comportamientos donde la violación de la norma se establece a partir del contenido que se difunde o se transfiere a través de internet.

El segundo grupo de cibercrimenes estudiados por LLINARES y que en buena parte de su obra aplica para exponer las transformaciones que el ciberespacio ha generado en los elementos del delito, se encuentra vinculado categóricamente al aspecto criminológico, como conductas que se desvían de lo normalmente aceptado por la sociedad y que atentan contra la integridad de esta. Refleja tres atributos a saber: cibercriminalidad social, política y económica. El autor sugiere una continua manifestación de los cibercrimenes sociales, por la interacción social en el ciberespacio, multiplicando la probabilidad de comportamientos lesivos que en el mundo físico se reducían considerablemente.

Frente a la cibercriminalidad económica MIRO LL., Fernando[63] sostiene que en tanto se generó un crecimiento exponencial de las tecnologías de la información y las comunicaciones, y la información contenida en los ordenadores y transmitida a través de la red cobra un valor económico significativo al punto de ser objeto de transacciones, se convirtió en el ápice del delito económico fundamentalmente cuando del fraude se trata.

> Cuando el protagonismo lo tuvieron las terminales informáticas y la información personal que ellas podían contener, aparecieron nuevas formas de afectar a la intimidad de las personas; cuando dichas terminales y la información en ellas contenida comenzaron a tener valor económico y a servir para la realización de transacciones económicas, surgieron las distintas formas de

[63] MIRO LL., Fernando. Delincuencia asociada al uso de las TIC. FUOC. Fundación para la Universitat Oberta de Catalunya, febrero 2013, p. 8, CC-BY-NC-ND • PID_00195950

> criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático, que, a su vez, evolucionó hacia el *scam*, el *phishing* y el *pharming* cuando apareció Internet; finalmente, con la universalización de la Red y la constitución del ciberespacio, comenzaron a surgir nuevas formas de criminalidad que aprovechaban la transnacionalidad de Internet para atacar intereses patrimoniales y personales de usuarios concretos, pero también para afectar a intereses colectivos por medio del ciberracismo o del ciberterrorismo.

A manera de síntesis, la obra Fenomenología y criminología de la delincuencia en el ciberespacio incluye una primera parte sobre la fenomenología del cibercrimen, donde analiza la criminalidad en el ciberespacio, siendo la diferencia entre cibercrimen y cibercriminalidad, la evolución del fenómeno, los sentidos psicológicos y normativos, su concepción amplia y restringida y la relación con el término cibercriminalidad. También aborda los tipos de cibercrimen y clasificación de los mismos, atendiendo a la incidencia de las tic en el comportamiento criminal, tales como: ciberataques puros; ciberataques réplica; ciberataques de contenido. Igualmente incluye otra explicación posible atendiendo al móvil y contexto criminológico, donde destaca el cibercrimen económico: la simbiosis de los ciberataques con finalidad económica; el cibercrimen social en la Web 2.0: redes sociales, desarrollo de la personalidad en el ciberespacio y nuevos cibercrimenes; el cibercrimen político: ciberterrorismo, ciberguerra y ciberhacktivismo. Por otra parte, aborda el cibercrimen y sus perfiles de

delincuentes en el ciberespacio, así como la cibervíctima, perfiles de victimización y riesgo real de la amenaza del cibercrimen.

Sobre la obra de MIRO LL., Fernando, Constanza di Piero comenta que ésta comprende y se comparte la decisión tomada por el autor de aplazar el análisis dogmático de los delitos informáticos, y adentrarse al desarrollo del fenómeno del cibercrimen desde una perspectiva criminológica (p. 17). Dar cabida a un análisis jurídico, sin el trabajo previo de investigación que ha realizado MIRÓ LLINARES, adolecería de rigor científico; toda vez que no se comprenderían las posibles dificultades jurídicas que la sociedad de la tecnología plantea, sino que tampoco podrían trazarse propuestas dogmáticas y soluciones políticocriminales acordes con los problemas. Precisamente, es lo que ha ocurrido, por ejemplo, con la tipificación del online grooming en España introducido por el legislador en la reforma operada por Ley Orgánica 5/2010, del 22 de junio. Se ha intentado dar una respuesta políticocriminal con notorio desconocimiento criminológico de los elementos configuradores, tanto del ámbito en el que se desarrolla el delito, como el de sus autores. Se resalta esta cuestión, por un lado, por la criminalización que ha sufrido el grooming virtual, y por el otro, por la relevancia dogmática y políticocriminal que poseen los delitos sexuales cometidos contra menores de edad. El legislador criminaliza, en aras de la importancia y de la efectiva protección del bien jurídico, determinados comportamientos que se encuentran situados en un estadio anterior de la concreta lesión del bien jurídico, e incluso posterior, como es el caso de la tenencia de pornografía infantil. Y paralelamente,

la doctrina se encuentra compelida a ahondar en la laboriosa necesidad de legitimar esas conductas[64].

H. Los ciberdelincuentes

Los ciberdelincuentes son aquellos que usan teléfonos móviles, computadoras portátiles o servidores de red para cometer un delito cibernético. Para estos delincuentes, las computadoras proporcionan los medios para cometer delitos. Por ejemplo, un ciberdelincuente puede piratear una red informática para diseminar un virus informático. O un delincuente puede usar una computadora para enviar pornografía infantil a otro usuario o suplantar la identidad de otra persona. Un delincuente comete un delito informático cuando utiliza una computadora como herramienta para cometer un delito. Aunque un delincuente no necesita habilidades informáticas especiales para cometer un delito informático, generalmente necesita tener un nivel más que básico de conocimiento informático para cometer un delito informático[65].

I. Terrorismo cibernético

El ciberterrorismo es el uso de Internet por parte de grupos terroristas que intentan afectar las políticas de una nación. Según lo definido por la Agencia Federal para el Manejo de Emergencias, el ciberterrorismo se relaciona con amenazas y

[64] DI PIERO, Constanza. Recensión a MIRÓ LLINARES, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, Universidad de Navarra, Barcelona, Julio de 2013

[65] Sadeghi, S. H. Pathology of learning in cyber space: Concepts, structures and processes. Springer International Publishing.2019, Vol. 156, pp 1-112 [Traducción en línea]

ataques ilegales contra computadoras, redes y la información almacenada en ellos, cuya acción es usar la tecnología para intimidar o coaccionar a un gobierno o su población en cumplimiento de objetivos políticos, sociales o de seguridad[66].

La infraestructura de información está cada vez más vulnerable frente al ataque de los ciberdelincuentes. La frecuencia, el costo y la sofisticación de los ataques están aumentando a tasas alarmantes. Amenazan la dependencia sustancial y creciente del comercio, los gobiernos y el público sobre la infraestructura de información para realizar negocios, llevar mensajes y procesar información. Algunas formas de ataque también representan una amenaza creciente para el público y las infraestructuras críticas para la prestación de servicios fundamentales para bienestar de la población[67].

Se ha dicho mucho sobre la amenaza que representa el delito cibernético, incluido el terrorismo, pero se ha hecho poco para proteger contra lo que se ha convertido en la forma más costosa de dicho delito: los ataques transnacionales a las computadoras y la infraestructura de la información. Las medidas adoptadas hasta ahora por los sectores público y privado no proporcionan un adecuado nivel de seguridad contra estos ataques considerando que Internet y otros aspectos de la infraestructura de información son inherentemente transnacionales, lo cual reclama una respuesta de la comunidad internacional lo suficientemente proactiva,

[66] HILL, J.B. y MARION, N.E. Op. Cit.

[67] GOODMAN, S.E. y SOFAER, A.D.Op. Cit.

para enfrentar estos desafíos transnacionales que representan una necesidad de solución inmediata y apremiante[68].

El desafío de controlar el delito cibernético transnacional requiere una gama completa de respuestas, incluida la cooperación tanto voluntaria como legalmente obligatoria de los países. Tanto el sector público como el privado ahora están buscando activamente iniciativas transnacionales, que van desde el intercambio voluntario e informal de información hasta un tratado multilateral como el propuesto por el Consejo de Europa –COF- para combatir el cibercrimen internacional mediante un compromiso mancomunado que implique un grado sustancial de cooperación en la investigación y el enjuiciamiento de tales crímenes.

Las declaraciones públicas y la cooperación internacional voluntaria, sin duda han ayudado a hacer frente a los ataques transnacionales. Se están asignando recursos para colocarlos a disposición de los países para mejorar las capacidades tecnológicas del personal de las fuerzas del orden nacionales e internacionales involucrados en investigaciones cibernéticas, lo cual, gracias a la cooperación internacional, se han rastreado algunos ataques y se han castigado a algunos perpetradores del ciberdelito trasnacional. Sin embargo, los pronunciamientos públicos, los programas educativos y la cooperación voluntaria no son suficientes, pues dar con las fuentes perpetradoras de ataques transnacionales nunca se ha determinado con exactitud, lo cual ha generado que muchos de ataques más

[68] Ibid. pg.45

dañinos, incluso cuando se identifican, quedan en la impunidad. Además, existe una gran disparidad entre la capacidad legal y tecnológica de los Estados para enfrentar los desafíos de prevenir, investigar y enjuiciar el delito cibernético, especialmente de carácter trasnacional[69].

J. El delito informático y el derecho

El delito informático, considerado como una amenaza internacional para la comunidad de países, aún adolece de medidas contundentes que permitan hacer un frente común para combatirlo, penalizarlo, o al menos prevenir las amenazas y riesgos que corre la sociedad, las personas y las organizaciones en general. Esta situación, en parte se ha debido a los esquemas jurídicos tomados desde cada Estado en particular, lo cual limita las acciones frente a lo heterogéneo de sus manifestaciones transfronterizas, afectando negativamente la eficacia de la tutela judicial, los procedimientos y demás garantías procesales, tal como lo señala FLORES P[70].al afirmar que:

> La lucha jurídica contra este tipo de criminalidad se asienta todavía hoy, en gran medida, sobre un esquema penal y judicial nacional, territorialmente limitado y heterogéneo. Ello explica la aparición frecuente de procedimientos penales paralelos y de conflictos internacionales de jurisdicción, que afectan negativamente a la eficacia de la tutela judicial, a la duración de

[69] VARGAS, J.,BAHNSEN, A. C.,VILLEGAS, S.,INGEVALDSON, D.Op.Cit. p. 58

[70] FLORES P., I. Criminalidad informática: aspectos sustantivos y procesales. Madrid-España: Tirant Lo Blanch, 2012, p.17

> los procedimientos y a las garantías procesales, muy señaladamente al principio de *non bis in ídem.*

Con la aparición del Internet, la informática, las redes sociales y las TIC en todas sus manifestaciones de la vida social, económica, cultural y de interacción, el derecho penal y sus procesos también requieren una actualización para hacer frente a la complejidad del ciberdelito, especialmente porque en su esencia siempre se había construido sobre la base de un modelo de delincuencia física, marginal e individual, lo cual lo convierte en una situación un tanto obsoleta frente a la criminalidad del mundo globalizado, dado que en la actualidad se presentan grandes dificultades para la detección y persecución del delito por su comisión de manera anónima, la proliferación de diferentes medios que afectan la seguridad de las personas y por el carácter transnacional de las conductas delictivas. Al respecto, BARRIOS A[71]., corrobora esta argumentación, al decir que:

> El Derecho Penal y Procesal penal clásico, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de delincuencia física, marginal e individual. Sin embargo, la aparición de la informática primero y de Internet después ha resquebrajado este paradigma, al tiempo que los distintos organismos encargados de su represión se han ido enfrentando a un cauce de ejecución criminal capaz de cuestionar muchos de los principios tradicionales de la investigación penal.

[71] BARRIOS A., M.Op. Cit. p.20

La comunidad internacional y los países enfrentan grandes desafíos en materia de persecución y represión de la criminalidad a través de medios informáticos, no sólo por la amenaza del terrorismo, sino también otro tipo de delitos con mayor impacto como lo son: el tráfico de estupefacientes, la venta de armas, la trata de personas, el blanqueo de capitales, entre otros, los cuales se cometen fuera de las fronteras y, por lo tanto, se vuelven inútiles las acciones tomadas por un Estado de manera particular, hasta tanto no se cuente con verdaderas medidas de colaboración en materia de manejo de la información y la cooperación interestatal para hacer frente al flagelo del ciberdelito.

A nivel de los países de la comunidad económica europea se señala una serie de acciones conjuntas para poder enfrentar el delito informático, el terrorismo, la trata de personas, el lavado de capitales, el narcotráfico, entre otros, y esto sólo es posible en la medida que exista estrecha colaboración entre los países, especialmente en la generalización del derecho penal de excepción y otras medidas como bien lo señala GONZÁLEZ C[72]., cuando señala:

> En el campo del derecho procesal, han de destacarse las problemáticas relativas a: a) competencia y jurisdicción: aplicación extraterritorial de la ley penal; cooperación internacional; extradición y euroorden; b) medios de investigación y prueba: interceptación de comunicaciones; diligencia de entrada y registro y confiscación de discos duros; registro y decomiso de datos

[72] GONZÁLEZ C., J. Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y la comunicación. Valencia, SPAIN: Editorial Tirant Lo Blanch, 2013, p. 233

> informáticos almacenados; recogida en tiempo real de datos informáticos; interceptación de datos relativos al contenido; interceptación de datos externos o de tráfico; c) responsabilidad del *service provider*. No debe desmerecerse el plano organizativo, es decir, la creación y reforzamiento de los órganos judiciales, fiscales y policiales especializados en la investigación y enjuiciamiento de estos delitos. Sin lugar a dudas se constata una tendencia a conservar e incrementar medidas excepcionales de carácter procesal en el enjuiciamiento del crimen organizado. Este conjunto de medidas especiales confirma una tendencia de la legislación penal hacia lo que ha venido llamándose la generalización del Derecho penal de excepción.

Como se planteó anteriormente, la globalización y las transformaciones económicas que la explican han hecho posible la aparición, el desarrollo y la masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictivas que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra a elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales[73].

Como complemento a lo anterior ROMEO C[74]. considera que:

[73] FLORES P., I.Op. Cit.

[74] ROMEO C., Carlos María. De los delitos informáticos al cibercrimen: En Universitas vitae homenaje a Ruperto Núñez Barbero. Ediciones Universidad de Salamanca, 2014, p. 655

> La pluralidad y diversidad de bienes jurídicos que pueden verse comprometidos, así como de medios comisivos, han impuesto la configuración en el Derecho comparado de una pluralidad de «delitos informáticos» y no de uno solo. En cualquier caso, ni la denominación de «delito informático», ni la de «delitos informáticos» (en todo caso preferible) apenas aportan en la actualidad una mínima precisión desde el punto de vista criminológico, dogmático, político-criminal y de política legislativa.

Para SUÁREZ SÁNCHEZ[75], analizando algunas variables frente a la "técnica legislativa para la regulación del delito informático", refiere:

> Las acciones propias de la criminalidad informática lesionan no sólo un grupo de intereses que pueden ser aglutinados en un único bien jurídico, pues afectan intereses de diversa índole que si bien es cierto que pueden dar lugar a parcelas que facilitan la reconducción a diversos bienes jurídicos (cualquiera que sean sus denominaciones y la entidad de las relaciones sociales que protejan), no es posible hacinarlas en un solo conjunto de intereses, pues sabido es que existe una gran diferencia entre las relaciones sociales que se protegen mediante las descripciones típicas, de los delitos contra el patrimonio, la fe pública, la intimidad, etc.
>
> El autor opina que la reforma penal vinculada a las modernas tecnologías de la informática y la comunicación debe tener una fórmula mixta, que describa tipos penales autónomos que tengan como finalidad proteger la informática, mediante la descripción de

[75] SUÁREZ SÁNCHEZ, Alberto. La Estafa Informática. Grupo Editorial Ibáñez, 2015. p. 52-53

> conductas que por lo general son peligrosas para el correcto funcionamiento del sistema informático, a fin de evitar la lesión a un bien jurídico concreto que tutele la informática, sin incurrir en la perdida de la perspectiva del bien jurídico que se desea tutelar, y la protección excesiva mediante tipos penales laxos de peligro abstracto, lo que implicaría riesgos para la seguridad jurídica y la superación de los límites de la intervención mínima al que ha de sujetarse el Derecho penal moderno, y modificar, adicionar y complementar los tipos penales ya existentes que protegen bienes jurídicos tradicionales, los que pueden ser realizados a través de sistemas informáticos o telemáticos[76].

Los antecedentes descritos a nivel internacional como nacional, reflejan la importancia de un tratamiento analítico de revisión de literatura pertinente a fin de generar nuevo conocimiento para el debate, el análisis y la modernización de la jurisprudencia en este campo tan amplio y tan desafiante para la sociedad y el mundo en general.

Ahora bien, la proliferación del ciberdelito como consecuencia del uso de las TIC, el Internet, las redes sociales y demás medios informáticos en el ciberespacio, trae un problema para los Estados y la comunidad internacional de países, por cuanto los delitos que a diario se cometen se realizan con total libertad e independencia del territorio, es decir, en múltiples jurisdicciones, originando grandes problemas para su detección, aplicación de la ley y prevención, entre otros. Desde el punto de vista del derecho, en la esfera penal, jurisdicción y ley

[76] SUÁREZ S., A., La Estafa Informática. 2015. Op. Cit.p. 53 - 54

aplicable al delito, no siempre estas coinciden con arreglo al derecho Penal de un Estado, lo cual genera zonas de impunidad frente al ciberdelito. Al respecto, sobre la complejidad para identificar la comisión de delitos, DÍAZ G[77]., señala que:

> Recordemos, el sujeto activo puede cometer sin problemas un delito desde un Estado diferente al que se encuentra el sujeto pasivo, incluso sin saber dónde se halla éste último. Esta nueva perspectiva, genera dudas a todos los niveles, tanto en relación al órgano estatal que va a conocer del asunto, como de la posibilidad de ejecutar la resolución recaída. Igualmente, un problema importante será la distinta regulación del Derecho sustantivo en los distintos Estados.

Por las consideraciones analizadas anteriormente, es importante centrarse en Colombia con respecto a la transferencia no consentida de activos, como un tipo de delito muy frecuente que merece ser analizado a la luz de la jurisdicción colombiana, pero también haciendo alusión al derecho comparado sobre este tema.

En la sociedad del conocimiento y de las TIC, han revolucionado todos los ámbitos de la sociedad, las organizaciones y las entidades estatales, así como las de contexto global. Las TIC y el Internet han generado una verdadera revolución hasta llegar a configurar lo que hoy se conoce como el ciberespacio virtual.

[77] DIAZ G., A. Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos. 2010, p.175

El Internet, actualmente hace parte de la vida cotidiana de las personas, los gobiernos y las organizaciones en general, por cuanto se presenta en todas las relaciones económicas, sociales y culturales, donde las redes sociales y la interacción del ciberespacio, constituyen actividades cotidianas y permanentes que han generado gran impacto en la sociedad actual y posiblemente en el corto, mediano y largo plazo. Al respecto BARRIOS A[78]., afirma que:

> El Internet se ha consolidado como pieza estructural de la Sociedad de la Información y desempeña un papel crucial en el desarrollo económico. La popularización de la Red a escala global ha permitido la creación del «ciberespacio virtual», tal y como lo concibiera el autor que acuñó tal término, William GIBSON[79], al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la última década del siglo XX, ha modificado las relaciones económicas, políticas, sociales y, muy especialmente, las personales.

Sobre la importancia de las TIC y el Internet que han permeado el mundo globalizado en el ámbito económico, social, cultural, medioambiental y principalmente financiero, su utilización es imprescindible por parte de la sociedad,

[78] BARRIOS A., M. Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015. España: Editorial Reus S.A., 2018, p. 9

[79] El prefijo cyber proviene, a su vez, del término cyberspace creado por el novelista de ciencia ficción William GIBSON y su obra Neuromancer (Editorial AceBooks, Nueva York, 1984), en la que el autor describía una sociedad tecnológicamente avanzada donde las personas vivían en un mundo virtual separado del mundo real. Citado por (Barrios A., 2018)

pero también infiere en las decisiones políticas y geoestratégicas de los gobiernos. Al respecto, FLORES P[80]., comenta:

> El Internet ya ocupa un espacio creciente en el mundo económico, comercial y financiero, en el que las transacciones, los acuerdos y los movimientos de capitales, bienes y servicios circulan a velocidad de la luz convertidos en combinaciones de bits. De igual modo, la Red se apropia cada vez a mayor velocidad de los canales de información, de las telecomunicaciones, de las comunicaciones interpersonales, de la oferta de ocio, cultura, arte, de la actividad científica, de la difusión del pensamiento, de los medios informativos, incluso de la política, amenazada en su concepción tradicional por la posible implantación de cibervoto y las consultas vinculantes a través de Internet.

Hasta aquí, se han presentado las bondades, ventajas e impactos positivos de las TIC, el Internet, las redes sociales y su influencia descollante en la sociedad actual. Sin embargo, a la par del desarrollo tecnológico, también han proliferado una serie de amenazas y riesgos para la seguridad de los países, de las personas y de las organizaciones, por cuanto el ciberdelito, el terrorismo y la consolidación de mafias internacionales, son un enemigo permanente en el ámbito de la

[80] FLORES P., I. Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. En: Revista Electrónica de Ciencia Penal y Criminología. 2015. vol. 17, no. 20, p. 4-5

comunidad internacional. Sobre esta aseveración, OJEDA y otros[81] plantean lo siguiente:

> Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica delitos informáticos, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática

Frente a la situación descrita, los países y la comunidad internacional ven la necesidad de establecer un frente común para realizar acciones conjuntas en pro de combatir el delito informático y la cibercriminalidad, obligando a la academia y las ciencias sociales en general, a reinterpretar la sociedad e identificar riesgos latentes, que merecen ser tratados dentro de cada jurisdicción, pero también en el ámbito internacional "el fenómeno de la criminalidad informática no es sólo de las grandes potencias, porque la utilización nociva de la informática afecta a todos los pueblos en donde se ha incorporado el computador como una herramienta de trabajo; desde luego, tal utilización perversa puede afectar a unas comunidades más que a otras"[82]

---

[81] OJEDA P., J., ARIAS F., M., RINCÓN R., F. y DAZA M., L. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 43

[82] SUÁREZ SÁNCHEZ, Alberto. La Estafa Informática. En: Derecho Penal y Criminología. 2006. vol. 27, p. 197

En este contexto, la información y la protección de los datos como bien jurídico, cobra vigencia por cuanto la mayor cantidad de delitos actualmente están relacionados con el manejo de la información y su intercambio a través de redes informáticas, constituyendo una amenaza y alto riesgo para la sociedad. Al respecto, MIRO L[83]. dice:

> El tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del cibercrimen, no ha terminado todavía ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas.

K. Marco Jurídico

Así como la globalización ha incursionado en todos los ámbitos de la sociedad y de la comunidad internacional, los delitos informáticos y el terrorismo a través del Internet, las redes sociales y los sistemas informáticos, también han impactado en el ámbito nacional e internacional, de allí la necesidad de abordar cuales han sido las medidas implementadas por algunos de los países más desarrollados frente a su seguridad, la prevención del delito y la sanción del mismo. La siguiente tabla, muestra los referentes a nivel de países sobre las acciones adelantadas para afrontar el delito.

[83] MIRO L., F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Revista electrónica de ciencia penal y criminología, 2012, p. 25

Tabla 1.Acciones tomadas para afrontar la Ciberdefensa a nivel de países

PAÍS	ACCIÓN TOMADA POR EL GOBIERNO
ALEMANIA	En febrero de 2011, el gobierno alemán lanzó su Estrategia de Seguridad Cibernética. En abril de 2011 el Ministerio del Interior puso en marcha el Centro Nacional de Ciberdefensa.
AUSTRALIA	Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio.
CANADÁ	El Departamento de Seguridad Pública implementó el Centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), y en octubre de 2010 adoptó la Estrategia Canadiense de Seguridad Cibernética.
ESTADOS UNIDOS	Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés), DHS: National Cyber Security División, US-CERT: United States Computer Emergency Readiness Team y la oficina de Seguridad Cibernética de la Casa Blanca. En mayo de 2011 fue adoptada la Estrategia Internacional para el Ciberespacio.
ESTONIA	En 2008 creó conjuntamente con otros países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciber amenazas. En este mismo año es adoptada una Estrategia de Seguridad Cibernética.
FRANCIA	Creó la Agencia de Seguridad para las Redes e Información (ANSSI), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. En febrero de 2011 fue adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información.

Fuente: Tomado de CONPES[84]

[84] Conpes 3701 de 2011 "Lineamientos de política para la Ciberseguridad y Ciberdefensa"

La interdependencia de los países dentro de la comunidad internacional también ha producido algunos referentes de organismos como las Naciones Unidas y los diferentes protocolos, donde se han analizado la necesidad de establecer convenios para combatir la ciberdelincuencia mediante la incorporación de las legislaciones internas, los lineamientos orientados a la prevención de las conductas delictivas. La siguiente tabla muestra dichos avances.

Tabla 2.Referentes normatividad internacional en seguridad informática

INSTRUMENTO	MATERIA
Convenio sobre Ciberdelincuencia[85] del Consejo de Europa – CCC (conocido como convenio sobre cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. Único instrumento vinculante vigente sobre el tema en el ámbito internacional y su protocolo para la criminalización de actos de racismo y xenofobia cometidos a través de sistemas informáticos. El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio[86] y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo.

[85] Acciones ilícitas que han sido cometidas mediante la utilización de un bien o servicio informático (Ministerio de Defensa Nacional de Colombia)

[86] Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética.(Academia de la Lengua Española)

Resolución AG/RES 2004 (XXXIV- O/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Estipula tres vías de acción: – Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores - CSIRT[87]. Este cometido fue asignado al Comité Interamericano Contra el Terrorismo - CICTE. – Identificación y adopción de normas técnicas para una arquitectura segura de Internet. Esta labor es desarrollada por la Comisión Interamericana de Telecomunicaciones. – Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.

Fuente: Tomado de CONPES[88]

Otros referentes internacionales a nivel de los países de la comunidad andina de naciones, también se han preocupado por establecer lineamientos en materia de seguridad y combate al delito informático. Igualmente la Unión Internacional de Telecomunicaciones y la ONU han emitido diferentes decisiones en esta materia, tal como se muestra en la siguiente tabla.

INSTRUMENTO	MATERIA
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004.	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones

[87] Por sus siglas en inglés: Computer Security Incident Response Team o Equipo de Respuesta a Incidentes de Seguridad Cibernética (www.first.org).

[88] CONPES, Op. Cit.

	orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad17 de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005.	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.
Resolución 64/25 “Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional” Asamblea General de las Naciones Unidas. (2009).	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información Esta resolución continúa el seguimiento de la Asamblea, con las resoluciones 53/70, de 4 de diciembre de 1998; 54/49, de 1° de diciembre de 1999; 55/28, de 20 de noviembre de 2000; 56/19, de 29 de noviembre de 2001, 57/53, de 22 de noviembre de 2002; 58/32, de 8 de diciembre de 2003; 59/61, de 3 de diciembre de 2004; 60/45, de 8 de diciembre de 2005; 61/54, de 6 de diciembre de 2006; 62/17, de 5 de diciembre de 2007; y 63/37, de 2 de diciembre de 2008.

Fuente: Tomado de CONPES[89]

Otras normativas de carácter internacional sobre los delitos informáticos se derivan de otros organismos tales como la Organización de Cooperación y Desarrollo Económico OCDE, que abogó por una regulación para que las legislaciones de los países miembros incluyeran medidas tendientes a combatir la delincuencia informática, para lo cual se constituyó una Comisión *ad hoc* encargada de emitir un informe donde se consignarán los principales problemas sobre la delincuencia informática y las dificultades técnicas para su combate o control[90].

[89] Ibid. p.15
[90] SUÁREZ S., A., La Estafa Informática. 2015. Op. Cit.p. 65 - 66

Por otra parte, la Organización de las Naciones Unidas ONU, en el octavo Congreso celebrado en La Habana en 1990, emite la resolución No. 45/121, en la que se invita a los estados miembros a realizar una modernización de las legislaciones penales nacionales para combatir el delito informático. Posteriormente la ONU expide en 1994 un manual sobre la prevención y control del delito informático[91].

La Unión Europea también ha dado bastante importancia a la actividad informática, realizando estudios para su reconocimiento e impacto entre los programas denominados IMPACT (*Information Maket Policy Action Plan*), así como el estudio titulado COMCRIME-*Study*, en el cual se realiza un análisis sobre la situación del tratamiento de la criminalidad informática al tenor de la legislación penal de los países miembros de la Unión Europea, Estados Unidos y Japón[92].

Otro referente lo constituye el Consejo de Europa como organismo internacional que se ha preocupado por los delitos informáticos y la manera como repercute a nivel internacional, emitiendo varias recomendaciones con miras a armonizar las leyes nacionales con respecto a la criminalidad económica, “en cuyo concepto incluía la criminalidad informática (recomendación No. R (81)12, y también con relación a las exigencias de la prueba escriturar y la admisión de la

[91] Ibid.

[92] SUÁREZ S., A., La Estafa Informática. 2015. Op. Cit.p. 67-68

reproducción de documentos y grabaciones en ordenadores como tales (recomendación No. R(81)20"[93]

Finalmente, para completar los referentes internacionales orientados a combatir el delito informático y como complemento a lo anterior, es la Asociación Internacional de Derecho Penal (AIDP), la cual según SUÁREZ S[94]., es:

> Una organización no gubernamental integrada por destacados penalistas de todo el mundo, que dedicó el Coloquio preparatorio de su XV Congreso (del 5 al 7 de octubre de 1992, en Wurzburg) al estudio de "el delito informático y otros delitos contra la tecnología de información", en el que se elaboró la propuesta de la resolución que al final fue adoptada bajo el título: "las infracciones informáticas y otros delitos contra la tecnología de la información", en el Congreso que luego celebró dicha organización en Río de Janeiro del cuatro al 10 de septiembre de 1994.

Lo anterior, ha correspondido al marco jurídico internacional en esta materia de los referentes orientados a combatir el delito informático a nivel global.

L. El ciberdelito en el derecho comparado

En este gran aparte, se presentan análisis generales sobre las legislaciones existentes en diversos países desarrollados y en vías de desarrollo, con respecto al tratamiento del ciberdelito en cada una de las legislaciones internas, para

[93] Ibid. p. 69

[94] Ibid. p.71

establecer algunos avances y paralelos frente a la tipificación de diversos delitos, la protección del agente pasivo y las consecuencias penales sobre su comisión de diversos casos tipificados

L.1 EL ENTORNO LEGISLATIVO.

La ley de delitos informáticos incluye leyes relacionadas con delitos informáticos, delitos de Internet, delitos de información, delitos de comunicaciones y delitos tecnológicos. Si bien Internet y la economía digital representan una oportunidad significativa, también es un facilitador de la actividad criminal. Las leyes de delitos cibernéticos crean los delitos y sanciones por delitos informáticos. El cibercrimen describe ambos: delitos dirigidos a computadoras, tecnologías de comunicación de datos o información (TIC), y delitos cometidos por personas que usan computadoras o TIC. El cibercrimen es un problema global que requiere una respuesta internacional coordinada.

Antes de la promulgación de delitos específicos de cibercrimen, las autoridades han recorrido a una revisión tipificada de los delitos existentes para hacer frente a esta nueva forma de delito cibernético. Por ejemplo, el acceso no autorizado a información privilegiada privada, podría verse como análogo a la intrusión. Otros paralelismos con el deterioro de los datos se pueden encontrar al considerar el delito desde el punto de vista penal. Tal enfoque tenía la ventaja de ser visto como una extensión de la ley en lugar de una revisión radical.

Aunque los delitos contra la propiedad proporcionaron una analogía inmediata, tales esfuerzos se han complicado por la aplicación de las nociones tradicionales de propiedad a los datos de la computadora. Por ejemplo, en el derecho consuetudinario la información confidencial generalmente no se considera 'propiedad' a los efectos del hurto. Este mismo principio aplica para los datos de la computadora, una persona que accede pero no modifica los datos, generalmente no será responsable por el hurto, ya que no se le quitará la propiedad. En otros contextos, los tribunales tuvieron dificultades para determinar si los datos informáticos constituyen propiedad en absoluto; El éxito o el fracaso de la acusación dependen en gran medida de la redacción del estatuto particular[95].

L.2 ALEMANIA.

Según el Derecho Penal Alemán, algunas otras actividades relacionadas con los delitos mencionados constituyen delitos. Estos son: (i) preparación de una obtención o interceptación no autorizada de datos, Sec. 202 del Código Penal alemán; | (ii) manejo de datos robados, Sec. 202 del Código Penal alemán; (iii) violación de los secretos postales y de telecomunicaciones, Sec. 206 del Código Penal alemán; (iv) sabotaje informático, Sec. 303b del Código Penal alemán; (v) ciertos tipos de violación del Reglamento General de Protección de Datos de la UE con la intención de enriquecer o dañar) a alguien, el art. 84 del Reglamento General de Protección de Datos y Sec. 42 de la Ley Federal de Protección de

[95] CLOUGH, J. Principles of Cybercrime. Cambridge University Press, 2015

Datos de Alemania; y (vi) falsificación de evidencia digital, Sec. 269 y ss. del Código Penal[96].

Los delitos mencionados anteriormente no tienen una aplicación extraterritorial específica. Sin embargo, la aplicación del Código Penal alemán depende del "lugar del delito". De acuerdo con la Sec. 9 del Código Penal alemán, se considera que se ha cometido un delito en todos los lugares donde actuó el delincuente o en el que el resultado se produce o debería haberse producido de acuerdo con la intención del delincuente. Por lo tanto, los delitos mencionados serán aplicables tanto si el delincuente actuó en el territorio de Alemania como en el caso de que el delito afecte a los sistemas informáticos que se encuentran o se utilizan para los servicios prestados en Alemania, donde el delincuente actuó desde fuera de Alemania[97].

La ciberseguridad se rige por varias leyes en Alemania. La ley principal relacionada con la ciberseguridad es la Ley de Seguridad Informática alemana (IT-Sicherheitsgesetz) de 25 de julio de 2015, que modificó una serie de leyes, en particular la Ley de Telemedia alemana (Telemediengesetz), la Ley de Telecomunicaciones alemana (Telekommunikationsgesetz), la General de la UE Reglamento de Protección de Datos (Datenschutz-Grundverordnung), la Ley Federal de Protección de Datos de Alemania (Bundesdatenschutzgesetz) y la Ley

[96] REICH, Pauline C, BRILL, Alan E, BALDWIN, Fletcher N y MUNRO, Robert John. Cybercrime & Security. West Publications, 2011, p. 245

[97] REICH, Pauline C, BRILL, Alan E, BALDWIN, Fletcher N y MUNRO, Robert John. Op. Cit.

de la Oficina Federal de Seguridad de la Información (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). Además de esto, partes de la ciberseguridad se rigen por la Ley Bancada (Kreditwesengesetz) y la Ley de Comercio de Valores (Wertpapierhandelsgesetz). Además de esta legislación formal, existen algunas disposiciones informales importantes con respecto a la seguridad informática en Alemania. Estos son los catálogos BSI Basic IT Protection desarrollados por la Oficina Federal de Seguridad de la Información (Bundesamt für Sicherheit in der Informationstechnik - BSI), los Criterios comunes para la evaluación de la seguridad de la tecnología de la información, estandarizados como ISO / IEC 15408 y los Objetivos de control para Información y tecnología relacionada (COBIT)[98].

L.3 FRANCIA.

La legislación de Francia en torno a la penalización de diversos delitos informáticos es muy amplia. Se relacionan solo los más importantes, tales como el hackeo (es decir, acceso no autorizado) o piratería es un delito penal de conformidad con el artículo 323-1 del Código Penal francés (FCC) relacionado con el acceso no autorizado a un sistema automatizado de procesamiento de datos. El castigo por el acceso fraudulento a un sistema automatizado de procesamiento de datos es el encarcelamiento y una multa de hasta € 60.000. Cuando los datos se modifican o suprimen como resultado del acceso no autorizado, la sanción es de tres años de prisión y una multa de hasta 100.000 €. Cuando el delito se comete en un sistema

[98] Ibid.

público o gubernamental, la sanción se eleva a cinco años de prisión y una multa de hasta € 150.000[99].

El delito de ataques de denegación de servicio, según el artículo 323-2 de la FCC sanciona el impedimento o la desaceleración de un sistema de información. Cualquier tipo de obstrucción dentro del perímetro del artículo 323-2 se castiga con cinco años de prisión y una multa de hasta € 150.000. Cuando el delito involucra un sistema público o gubernamental, las sanciones se elevan a siete años de prisión y una multa de hasta € 300.000[100].

La suplantación de identidad o phishing está sancionada por los siguientes artículos de la FCC y del Código de Propiedad Intelectual:

(i) la recopilación de datos por métodos fraudulentos, injustos o ilegales está sancionada por el artículo 226-18 de la FCC por cinco años de prisión y una multa de hasta € 300,000; el hurto y uso de una identidad de terceros está sancionado por el artículo 226-4-1 de la FCC por un año de prisión y una multa de hasta € 15.000: la sanción aplicada es acumulativa con las sanciones aplicadas de conformidad con el fraude o estafa está sancionado por el artículo 313-1 de la FCC por cinco años de prisión y una multa de hasta € 375.000; la introducción no

[99] CALDERONI, Francesco The European legal framework on cybercrime: striving for an effective implementation. En: Crime, law

[100] Ibid.

autorizada de datos en un sistema, la extracción, reproducción, transmisión y uso de los datos almacenados en este sistema está sancionada por el artículo 323-3 de la FCC por cinco años de prisión y una multa de hasta € 150.000; y (v) el phishing puede resultar en una infracción de los derechos de propiedad intelectual, en particular sobre la base de los artículos L.335-2, L.713-2 y L.713-3 del Código francés de propiedad intelectual. El propietario del sitio web o marca registrada reproducida o imitada puede demandar al phisher por el uso de su marca registrada por infracción. Este delito está sancionado con tres años de prisión y una multa de hasta € 300.000[101].

En cuanto al delito de posesión o uso de hardware, software u otras herramientas utilizadas para cometer delitos cibernéticos (de piratería). De conformidad con el artículo 323-3-1 de la FCC, el acto que consiste, sin un motivo legítimo (en particular para la investigación o la seguridad informática) en importar, mantener, ofrecer, transferir o poner a disposición equipos, instrumentos, programas informáticos o cualquier información diseñado o especialmente adaptado para cometer uno o más delitos mencionados en los artículos 323-1 a 323-3 de la FCC se castiga con las sanciones más severas[102].

El hurto electrónico (por ejemplo, abuso de confianza por parte de un empleado actual o anterior, o infracción penal de derechos de autor). Este delito de

[101] CALDERONI, Francesco. Op. Cit.

[102] CALDERONI, Francesco. Op. Cit.

apropiación ilícita de conformidad con la FCC (artículo 311-1) se ha extendido al hurto de computadoras por los tribunales franceses. Los jueces franceses ahora consideran los datos informáticos (es decir, la información desmaterializada), como elementos que pueden ser robados. Según la ley francesa, el hurto se castiga con tres años de prisión y una multa de hasta 45.000 €. El artículo 226-18 de la FCC, así como los artículos L.335-2, L.713-2 y L.713-3 del Código francés de propiedad intelectual también podría usarse en algunas circunstancias103.

L.4 ITALIA.

La legislación de Italia en torno a la penalización de diversos delitos informáticos, los más principales según ZICCARDI[104] son los siguientes:

Hackeo (es decir, acceso no autorizado). El acceso no autorizado a una computadora o sistema de telecomunicaciones (Artículo 615, Código de Derecho Penal). Este delito requiere que una persona obtenga acceso a una información protegida o sistema de telecomunicaciones contra el consentimiento expreso o implícito de la persona con derecho a excluir a terceros de obtener dicho acceso. El castigo es prisión hasta por tres años.

Fraude digital o fraude (Artículo 640, Código de Derecho Penal). Este delito ocurre cuando quien, a sabiendas y con la intención de defraudar, manipula uno o

[103] Ibid.

[104] ZICCARDI, Giovanni. Cybercrime and jurisdiction in Italy en Informatica giuridica. [traduccion digital]. En: Privacy, sicurezza informatica, computer forensics e investigazioni digitali. 2012, p. 324.

más dispositivos digitales, utilizando ilegalmente información, datos o software en un dispositivo digital, para ganar dinero y dañar a otra persona. El castigo es prisión de entre seis meses y tres años.

Identidad falsa (Artículo 494, Código de Derecho Penal). El artículo en cuestión es aplicable a identidades reales así como a identidades digitales; el delito relevante se perpetra cuando alguien se representa falsa y deliberadamente como otra persona. El castigo es prisión hasta por un año.

Posesión ilegal y difusión de contraseñas a sistemas digitales (Artículo 615 quater, Código de Derecho Penal). Este delito se perpetra cuando una persona tiene o difunde legalmente códigos de acceso secretos para ganar dinero o dañar a otra persona. El castigo es prisión hasta por un año.

Ataques de denegación de servicio, daño de la información digital, datos o software (Artículo 635 bis, Código de Derecho Penal). Esto ocurre cuando alguien daña, destruye, elimina o deshabilita intencionalmente cualquier tipo de información digital, datos o software que pertenezca a otra persona. El castigo es prisión de entre seis meses y tres años. Suplantación de identidad, fraude digital o fraude (Artículo 640, Código de Derecho Penal), identidad falsa (Artículo 494, Código de Derecho Penal), entre otros[105].

[105] ZICCARDI, Giovanni. Op. Cit.

L.5 AUSTRALIA

Australia ha sido parte en la Convención del Consejo de Europa sobre Ciberdelincuencia (la Convención de Budapest) desde 2013. Australia trabaja con países de la región interesados en adherirse a la Convención de Budapest, ayudándoles a lograr la reforma legislativa reglamentada.

Sobre los delitos informáticos, algunos apartes de la legislación de Australia tipifican varios delitos relacionados con el acceso no autorizado, la modificación y el deterioro de los datos. Estos delitos se dividen en "delitos informáticos graves" (División 477) y "otros delitos informáticos" (División 478). La interceptación de las comunicaciones se trata en una legislación separada. Aunque está destinado a proporcionar un modelo para todas las jurisdicciones, el Código Penal no se ha adoptado ampliamente. En consecuencia, los delitos cibernéticos australianos son un mosaico de jurisdicciones, algunas adoptan sus propios enfoques mientras que otras acatan las normas generales[106].

El poder legislativo de la Commonwealth en relación con las telecomunicaciones le otorga un amplio mandato legislativo en esta área. Según esta disposición, es un delito conectar equipos o utilizar equipos conectados a una red de telecomunicaciones con la intención de cometer o facilitar la comisión de una infracción grave.

[106] HOOPER, Christopher, MARTINI, Ben y CHOO, Kim-Kwang Raymond Cloud computing and its implications for cybercrime investigations in Australia. En: Computer Law

Siempre y cuando la red se utilice para facilitar o cometer un delito de este tipo, el delito está oculto. Tampoco es necesario demostrar que el delito grave se facilitó realmente; de hecho, el delito puede extenderse incluso cuando sea imposible cometer el delito grave. Es suficiente que el acusado tenga la intención de facilitar el delito. Por lo tanto, castiga el conducto preparatorio que puede estar muy por debajo de la ley de intentos[107].

La Commonwealth, no solo se superpone potencialmente con las leyes estatales (aunque es poco probable que la Commonwealth haya manifestado la intención de cubrir el campo), sino que puede desplazar delitos más específicos de la Commonwealth, como los relacionados con el acceso no autorizado a las computadoras con la intención de cometer una infracción grave. Estos problemas se ven exacerbados por su aplicación a las leyes extranjeras.

Más recientemente, una serie de restricciones jurisdiccionales fueron eliminadas de los delitos informáticos de la Commonwealth por la Ley de Enmienda de Legislación de Cibercriminal 2012 (Cth). Inicialmente necesarios para proporcionar al gobierno poder federal por delitos informáticos. Sin embargo, con la adhesión de Australia a la Convención sobre Delitos Cibernéticos, la Commonwealth se basará en el poder de los "asuntos externos" para proporcionar delitos integrales de delitos informáticos. Aunque estos se superpondrán en gran

[107] HOOPER, Christopher, MARTINI, Ben y CHOO. Op. Cit.

medida con las disposiciones estatales y territoriales, la intención de la Commonwealth no es para 'cubrir el campo', por lo tanto conservando la validez de las leyes estatales inconsistentes[108].

L.6 CANADÁ.

La reforma del Código Penal canadiense para abordar los problemas del uso indebido de la computadora surgió en gran medida como resultado de la decisión de la Corte Suprema en McLaughlin. Un proyecto de ley fue remitido al Comité Permanente de Justicia y Asuntos Legales de la Cámara, que presentó su informe el 29 de junio de 1983[109]. El Comité rechazó la idea de un estatuto de delito cibernético específico sobre la base de que tal estatuto tomaría demasiado tiempo para redactarse, y que el delito cibernético no debería ser tratado de manera diferente a otros tipos de delitos. Por lo tanto, el Comité recomendó enmiendas al Código Penal, adoptando un enfoque de dos niveles, con un delito de acceso no autorizado y otro de alteración o destrucción no autorizada de datos de la computadora. Estas enmiendas entraron en vigencia el 4 de diciembre de 1985, y fueron complementadas en 1997 por la Ley de Mejora del Derecho Penal, que introdujo un delito de tráfico de contraseñas y dispositivos informáticos utilizados para cometer delitos cibernéticos[110]

---

[108] Ibid.

[109] LEVIN, Avner y GOODRICK, Paul From cybercrime to cyberwar? The international policy shift and its implications for Canada. En: Canadian Foreign Policy Journal. 2013. vol. 19, no. 2, p. 127-143

[110] Ibid.

L.7 EL REINO UNIDO

Una vez que comenzó la reforma a la legislación sobre el delito informático en el Reino Unido, ésta se produjo rápidamente. La Comisión de Derecho publicó tanto su Documento de trabajo como el Informe final sobre "Uso indebido de la computadora" con un año de diferencia. Esto fue seguido en 1990 por la promulgación de la Ley de uso indebido de computadoras de 1990 (Reino Unido). La Ley inicialmente penalizó dos formas de conducta: 'acceso no autorizado a material informático' (artículos 1 y 2) y 'modificación no autorizada de material informático' (s. 3). Tras una revisión realizada por el Grupo Parlamentario de Internet de todos los Partidos (AP1G), la Parte 5 de la Ley de Policía y Justicia de 2006 (Reino Unido) realizó algunas reformas importantes. Estas enmiendas intentaron abordar algunos de los problemas específicos que habían surgido bajo la ley existente, particularmente en relación con los ataques DoS, y también para cumplir con el Convenio sobre Delitos Cibernéticos y la Decisión Marco de la UE. Las enmiendas también introdujeron un nuevo delito relacionado con el tráfico en 'hackear dispositivos'[111].

Más recientemente, se han promulgado cambios significativos en la Ley de uso indebido de computadoras como parte de la Ley de delitos graves de 2015 (Reino Unido). Estas reformas particulares surgieron de una revisión de la Ley, como se presagiaba en la Estrategia de Seguridad Cibernética. La primera reforma

[111] ALKAABI, ALI, MOHAY, GEORGE, MCCULLAGH, ADRIAN, CHANTLER, NICHOLAS. Dealing with the Problem of Cybercrime. Springer Berlin Heidelberg, 2011, ps. 1-18

significativa es la creación de un nuevo delito de actos no autorizados que causen o generen el riesgo de daños graves, que está destinado a abordar una brecha percibida en la ley donde la pena máxima por acceso no autorizado que causa impedimento es de diez años de prisión, independientemente del nivel de daño causado[112].

El segundo grupo de reformas surgió de la necesidad de cumplir con la Directiva de la CE sobre ataques contra sistemas de información. La Sección 3A, que se refiere al tráfico de herramientas de piratería, se modifica para incluir aquellas situaciones en las que el acusado obtiene herramientas para usar y cometer un delito en virtud de la Ley, independientemente de la intención de suministrar. Las reformas también ampliaron el alcance jurisdiccional del Reino Unido en relación con los delitos previstos en la Ley para cumplir con el artículo 12 de la Directiva[113].

L.8 ESTADOS UNIDOS.

El primer estatuto de delito informático de EE. UU se promulgó en Florida en 1978, y los 50 Estados ahora han seguido su ejemplo. Aunque la legislación federal se había propuesto anteriormente, la primera Ley federal fue la Ley de fraude y abuso de dispositivos para cometer fraude informático. Sin embargo, su alcance limitado y su falta de claridad significaron que pronto fue reemplazado por la Ley de Abuso

[112] ALKAABI, ALI, MOHAY, GEORGE, MCCULLAGH, ADRIAN, CHANTLER, NICHOLAS. Op. Cit.

[113] Ibid

y Fraude Informático de 1986 (CFAA), codificada en 18 USC § 1030. Este sigue siendo el principal estatuto federal de delitos informáticos, aunque su alcance se expandió significativamente para incluir 'computadoras protegidas', la difusión de malware y el tráfico de contraseñas de computadora. Es importante destacar que el CFAA también permite soluciones civiles, que ha contribuido significativamente a la jurisprudencia en esta área y, posiblemente, ha llevado a interpretaciones más expansivas que las que podrían ocurrir en los tribunales penales[114].

El Capítulo 3 se refiere al acceso no autorizado a las computadoras, mientras que el Capítulo 4 se centra en la modificación no autorizada o el deterioro de los datos. También son relevantes para esta categoría de delitos los delitos relacionados con el mal uso de dispositivos que pueden usarse para facilitar la comisión de estos delitos (Capítulo 5) y la interceptación no autorizada de datos (Capítulo 6)[115]

L.9 ESPAÑA.

Mediante la Ley Orgánica 10 del 23 de noviembre de 1995, las Cortes Generales y el rey de España aprobaron y sancionaron el Código Penal vigente, el cual incluye la tipificación de la delincuencia informática.

El delito informático con mayor pena de prisión en este país es la "Alteración, copia, reproducción o falsificación de tarjetas de crédito o débito o cheques de

[114] WINMILL, B Lynn, METCALF, David L y BAND, Michael E Cybercrime: Issues and challenges in the United States., 2010. En: Digital Evidence Elec. Signature L. Rev. 2010. vol. 7

[115] Ibid.

viaje; así como la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de la conducta referida" (las Cortes Generales y el rey de España, 1995).

España es un modelo de referencia en este campo. Debido a su condición de Estado miembro del Concejo Europeo, firmó el convenio del cibercrimen el 23 de noviembre del 2001, realizando su última ratificación el 3 de junio de 2010 y entrada en vigor el 1° de octubre del mismo año[116].

En relación con el delito cibernético, encontramos inclusiones parciales en el Código Penal, la Ley Orgánica 5/2000, de 12 de enero, que regula la responsabilidad penal de los menores; o en el Real Decreto que aprueba la Ley de Procedimiento Penal.

También es aplicable el reglamento sobre protección de datos, desarrollado por la Ley Orgánica 15/1999, de 13 de diciembre y sus reglamentos, aprobados por el Real Decreto 1720/2007 de 21 de diciembre. España forma parte del grupo de países de la Convención de Budapest sobre Cibercrimen de 2001, a la que se adhirió en 2010. El 5 de diciembre de 2013, el gobierno aprobó su Estrategia Nacional de Ciberseguridad, "destinada a enfrentar el enorme desafío que representa preservar el ciberespacio de los riesgos y amenazas que enfrenta". Los

[116] ROJAS PARRA, Jaime Hernán.Op. Cit. p.221

secretarios de Estado de seguridad y telecomunicaciones también han firmado un acuerdo para cooperar en la lucha contra el cibercrimen. Tanto la Guardia Civil como la Policía Nacional han puesto más recursos en unidades que luchan contra el crimen digital [117]

En cuanto a la ciberseguridad a nivel técnico y organizativo, España se rige por el nuevo Reglamento Europeo de Protección de Datos - Reglamento (UE) 2016/679, así como la existencia de otros tipos de protocolos o normas internacionales, especialmente los relacionados con la transferencia internacional de datos, como el Escudo de privacidad. Estas son solo algunas de las reglas que tienen como objetivo proteger el ciberespacio, pero hay muchas más detalladas que regulan aspectos aún más específicos.

Por ejemplo, las reglas que deben tenerse en cuenta al cometer un acto criminal relacionado con la suplantación de una marca o empresa, el uso ilegal de la misma o la infracción de creaciones de autores protegidos por propiedad intelectual. En estos casos, además de las normas que aparecen en el código español mencionado anteriormente, también es necesario tener en cuenta la ley de marcas o la normativa sobre propiedad intelectual e industrial, según corresponda. Por lo tanto, la ciberseguridad puede romperse no solo por la comisión u omisión de ciertos actos que tienen que ver con la seguridad en sí

[117] PRADILLO, Juan Carlos Ortiz Fighting against cybercrime in Europe: the admissibility of remote searches in Spain. En: Eur. J. Crime Crim. L.Crim. Just. 2011. vol. 19, p. 363

misma, sino que a veces el derecho de un tercero también puede verse afectado al aprovechar los actos que van específicamente contra la seguridad de una red[118].

Analizada la legislación de España en torno al ciberdelito y su comparación con el caso colombiano, hay similitudes frente al derecho penal y su aplicación punitiva en cuanto al delito informático, espacialmente en consideración a la transferencia no consentida de activos, contemplado en la Ley 599 de 2000, código penal de Colombiano.

Según la doctrina española, los delitos informáticos se subdividen en dos grupos: uno que puede ser aquel que atenta contra la intimidad de las personas ante el gran cúmulo de datos que mantienen en sus correos electrónicos, redes sociales o discos personales de sus computadores, y otro que se compone de aquellos que atentan contra el patrimonio económico, y que se cometen utilizando las nuevas tecnologías informáticas. Además, señala que los delitos contra el sistema informático se pueden catalogar como los "… referidos tanto a sus elementos físicos como lógicos, incluyendo aquí los delitos de hurto, hurto de uso, robo, apropiación indebida, estafa, daños…", así como "… los delitos cometidos "por medio" del sistema informático", distinguiendo a su vez, dentro de estos, aquellos en los que el uso del modo informático no es absolutamente necesario, pudiéndose cometer el delito por un medio no informático si el autor así lo hubiere

[118] PRADILLO, Juan Carlos. Op. Cit.

decidido, y los que únicamente pueden ser cometidos por medios informáticos. De este modo no solo concluye sobre cuáles son los delitos informáticos, sino también acerca de aquellos que se cometen contra los sistemas informáticos.

L.10 ARGENTINA.

Mediante la Ley 26388, de 4 de junio de 2008, se modifica la Ley 11179, Código Penal de la Nación Argentina, con el objeto de incorporar y sustituir del código referido varios artículos regulatorios de los delitos informáticos.

El Senado y la Cámara de Diputados argentinos, reunidos en congreso, sancionaron la sustitución del epígrafe del capítulo iii del título v del libro ii de su Código Penal, definiéndolo como "Violación de secretos y de la privacidad", el cual castiga y tipifica las conductas punibles como aparece a continuación:

El delito informático con mayor pena de prisión es "Defraudar con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de trucos o engaños, mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de sistemas informáticos" (Senado y Cámara de Diputados de la Nación de Argentina, 2008).

En marzo de 2010, Argentina se adhirió al Convenio sobre la Ciberdelincuencia por parte del Consejo de Ministros del Consejo de Europa.

Por otra parte, la regulación legal más completa con respecto a la protección de datos personales en Argentina es la Ley de Protección de Datos Personales (Ley de Protección de Datos), que está regulada por el Decreto N ° 1558/2001 y aplicada por la Autoridad de Protección de Datos (DPA).

El principio general bajo la Ley de Protección de Datos es que cualquier tratamiento de datos personales debe ser consentido específicamente por el interesado. Dicho consentimiento debe otorgarse libremente, en función de la información proporcionada previamente al interesado (informado) y expresada por escrito o por medios equivalentes, dependiendo de cada caso. El interesado puede revocar el consentimiento en cualquier momento, aunque esto no tendrá un efecto retroactivo.

En cuanto a la transferencia internacional de datos personales, está prohibido en el caso de países u organizaciones internacionales que no brinden un nivel adecuado de protección de acuerdo con los criterios de la DPA, a menos que: (i) el interesado haya otorgado expresamente su consentimiento; (ii) existe un acuerdo de transferencia internacional que proporciona el mismo nivel de protección; o (iii) el cesionario y el cedente están obligados a autorregularse. Además, el Reglamento No. 60-E / 2016 también proporciona una lista de países adecuados de la siguiente manera: Estados miembros de la Unión Europea y el Espacio Económico Europeo, Suiza, Guernsey y Jersey, la Isla de

Man, las Islas Feroe, Canadá (solo aplicable a su sector privado), Nueva Zelanda, Andorra y Uruguay.

El delito cibernético no ha sido regulado específicamente por la legislación Argentina. Durante algún tiempo, la falta de un esquema regulador favoreció a los ciberdelincuentes, ya que no podían ser procesados porque no existe un delito y, por lo tanto, no pueden ser castigados, a menos que la actividad esté expresa y específicamente codificada. Esto cambió en 2008 cuando el Código Penal fue modificado por la adopción de la Ley de Delitos Cibernéticos[119].

Al crear nuevas ofensas y también modificar ciertos aspectos de los procedimientos ya empleados en el país, con el objetivo de adaptarse a las nuevas formas de tecnología y los desafíos que planteaban, se aprobó la Ley de Delitos Cibernéticos sin ningún cambio crucial en la propuesta original. Esta ley, redactada siguiendo pautas similares establecidas por la Convención de Budapest sobre Cibercrimen, se alineó con las definiciones ya establecidas por la comunidad internacional, ayudando a la adopción de la ley.

La Ley de Delitos Cibernéticos fue un gran avance hacia la protección de la seguridad cibernética, pero no cubre todos los actos ilícitos que pueden cometerse. El resultado es que algunos delitos quedan impunes, dejando a las víctimas de delitos de ciberseguridad sin protección. Otra limitación de la ley es

[119] CATÁ DEL PALACIO, Arturo. Ciberdelincuencia. Desarrollo y persecución tecnológica. 2014

que no establece medidas legislativas que permitan establecer procedimientos penales específicos para la adquisición de pruebas electrónicas de cualquier tipo de delitos cometidos a través de un sistema informático, lo que genera problemas de aplicación.

SINOPSIS
Ley 26388 26/6/08 reforma del código penal argentino Contenido: . Pornografía infantil por Internet u otros medios electrónicos (Art. 128 CP); . Violación, apoderamiento y desvío de comunicación electrónica (Art. 153, párrafo 1o CP); . Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (Art. 153, CP); . Acceso a un sistema o dato informático (artículo 153 bis CP); . Publicación de una comunicación electrónica (artículo 155 CP); . Acceso a un banco de datos personales (artículo 157 bis, párrafo 1o CP); . Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2o CP); . Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2o CP; anteriormente regulado en el artículo 117 bis, párrafo 1o, incorporado por la Ley de Hábeas Data); . Fraude informático (artículo 173, inciso 16 CP); . Daño o sabotaje informático (artículos 183 y 184, incisos 5o y 6o CP) Técnica: Reforma código penal (La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia).

Fuente: Adaptado de GAMBA[120]

[120] GAMBA, Jacopo. Panorama del derecho informático en América Latina y el Caribe. En: CEPAL - Colección Documentos de proyectos. 2010, p. 1-44

L.11 BRASIL.

Para el caso de Brasil, tiene tipificados varios ciberdelitos, entre ellos, la piratería, la cual constituye un delito penal en virtud de la Ley No.737/2012. Esta Ley modificó la Disposición 154-A del Código Penal brasileño para establecer que la invasión del dispositivo informático de un tercero, esté o no conectado a una red informática, a través de una violación indebida de un mecanismo de seguridad y con el propósito de obtener, adulterar o destruir datos es un delito en Brasil. La pena máxima por dicho delito es un año de prisión y multa, o dos años de prisión y una multa si el pirata informático obtiene los contenidos de comunicaciones electrónicas privadas de la víctima, secretos comerciales o industriales, o información confidencial. Los dos años de prisión y una multa también se aplican si el pirata informático controla el dispositivo invadido de forma remota. Las sanciones antes mencionadas pueden incrementarse cuando existan circunstancias agravantes[121].

Además de la normatividad que se refiere a delitos penales, existen también disposiciones importantes relacionadas con los derechos civiles en la Ley de Internet de Brasil (Marco Civil da internet) y su Decreto reglamentario No. 771/2015. Además, la Constitución brasileña, el Código del Consumidor y la Ley de Propiedad Industrial tienen disposiciones dispersas relacionadas con temas

[121] MUGGAH, Robert y NATHAN, Thompson Brazil's Cybercrime Problem. En: Foreign affairs: Latinoamérica. 2015. vol. 17, p.1-7 [Traducción en línea]

que pueden estar relacionados con la ciberseguridad. Además, el Presidente de Brasil firmó la primera Ley de Protección de Datos de Brasil el 14 de agosto de 2018, que entrará en vigencia en febrero de 2020. Con respecto a esta Ley, las organizaciones deberán implementar medidas técnicas para salvaguardar los datos personales. Además, el Banco Central de Brasil emitió recientemente la Resolución N ° 4.658 / 2018, que entrará en vigencia el 31 de diciembre de 2021, sobre la adopción de medidas en el campo de la ciberseguridad[122].

Sobre la Ley de Protección de Datos de Brasil está la Autoridad de Protección de Datos como el Regulador. Sin embargo, el presidente brasileño vetó el capítulo dedicado a esta Autoridad debido a la falta de formalidad según lo solicitado por la Constitución brasileña. En vista de eso, la Autoridad de Protección de Datos no se incorporó a la Ley de Protección de Datos, pero el Presidente se compromete a proponer una ley específica para crear la Autoridad.

Se espera que esta Autoridad tenga poderes para regular la protección de datos, monitorear el cumplimiento de las empresas y las personas con la Ley de Protección de Datos e imponer sanciones en caso de incumplimiento de la Ley. Además, otros reguladores pueden supervisar el cumplimiento de las normas y estándares del sector (por ejemplo, el Banco Central de Brasil puede supervisar el

[122] MUGGAH, Robert y NATHAN, Thompson. Op. Cit.

cumplimiento de las instituciones financieras con su Resolución No. 4.658 / 2018)[123].

SINOPSIS
Ley 8137 (27/12/90), sobre “Crímenes contra el orden económico y las relaciones de consumo” ***Contenido*** Uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la Hacienda Pública. ***Técnica*** Ley especial **Ley 7646/1987** ***Contenido*** Violación de derechos de autor de programas de ordenador Acceso a bancos de datos. **Técnica** Ley especial **Ley 9100, Art. 67 inc. VII** ***Contenido*** Tipo penal para punir con reclusión de uno a dos años y multa la obtención indebida de acceso, o su intento, a un sistema de tratamiento automatizado de datos utilizado por el servicio electoral, con el fin de alterar el cómputo o cálculo de votos ***Técnica*** Ley especial

Fuente: Adaptado de GAMBA[124]

L12 PERÚ.

En Perú existe la Dirección de Investigación Criminal y de Apoyo a la Justicia, con su División de Delitos de Alta Tecnología, que es parte de la Policía Nacional del

[123] MUGGAH, Robert y NATHAN, Thompson. Op. Cit.

[124] GAMBA, Jacopo. Op. Cit.

Perú (PNP). Cuentan con tres departamentos: i) Departamento de Delitos Informáticos, Patrullaje Virtual, ii) Departamento de Investigación Especial (Hurto de Fondos, Pornografía Infantil, Piratería de Software, Investigaciones Especiales) y iii) Departamento de Coordinación, Coordinación Búsqueda de Información[125].

El 22 de octubre de 2007, el Congreso de la República de dicha nación emite la Ley 30096 o ley de delitos informáticos, la cual tiene por objeto prevenir y sancionar toda conducta ilícita cometida a través de la utilización de tecnologías de la información o comunicación que puedan llegar a afectar sistemas, datos informáticos y otros bienes jurídicos penalmente importantes[126].

Esta ley, cuya finalidad es luchar contra la ciberdelincuencia, consta de siete capítulos, a saber: "finalidad y objeto de la Ley", "delitos contra datos y sistemas informáticos", "delitos informáticos contra indemnidad y libertad sexuales", "delitos informáticos contra la intimidad y el secreto de las comunicaciones", "delitos informáticos contra el patrimonio", "delitos informáticos contra la fe pública" y finalmente "disposiciones comunes".

El 10 de marzo de 2014, el Congreso de la República del Perú emite la Ley 30171, la cual modifica la Ley 30096, ley de delitos informáticos, con el objeto de

[125] KSHETRI, Nir. Cybercrime and Cybersecurity in Latin American and Caribbean Economies. [Traducción en línea] En: Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan UK 2013, p. 135-151.

[126] Ibid.

incorporar la calidad de "deliberada" e "ilegítima" a las conductas delictivas, sancionadas en la tipificación de los delitos informáticos regulados[127].

Los delitos informáticos con mayor pena de prisión en la República del Perú son los siguientes:

- "Interceptación indebida de datos informáticos en transmisiones no públicas, dirigidas, originadas o efectuadas en sistemas informáticos o electromagnéticos, mediante el uso de tecnologías de la información o comunicación, que comprometa la defensa, la seguridad o la soberanía nacional" (Congreso de la República del Perú).

- "Fraude a través de las tecnologías de la información o comunicación, para diseñar, introducir, alterar, borrar, suprimir, clonar datos informáticos o cualquier interferencia o manipulación del funcionamiento de sistemas informáticos, para afectar el patrimonio del Estado destinado a fines asistenciales" (Congreso de la República del Perú)[128].

SINOPSIS
Ley 27309, ley de incorporación de los delitos informáticos al código penal *Contenido* Figuras: ingreso o interferencia en bases de datos, sistema o red de computadores. *Técnica* Ley especial de incorporación de los delitos informáticos en el código penal

[127] KSHETRI, Nir. Op. Cit.

[128] Ibid.

Proyecto de ley No. 2825-2000/CR, sobre pornografía infantil en Internet
Contenido El proyecto trata de tipificar e incorporar en el Código Penal el tipo penal de pornografía infantil que contemple tanto la conducta de procurar y facilitar que los menores de dieciocho años realicen actos de exhibicionismo corporal, lascivos y sexuales con el objeto y fin de fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, como la de fijar, grabar, imprimir, actos de exhibicionismo corporal lascivos y sexuales con menores de dieciocho años y la de elaborar, reproducir, vender, arrendar, exponer, publicitar o trasmitir el material pornográfico.

Fuente: Adaptado de GAMBA[129]

L.13 URUGUAY.

El Código Penal de la República Oriental de Uruguay es la única legislación que se relaciona con la tipificación de la delincuencia informática, aunque no se enuncian ni sancionan conductas penales cometidas a través de medios electrónicos, sistemas informáticos o programas de computación. El delito informático con mayor pena de prisión en Uruguay es la "Violación de correspondencia escrita, mediante apertura, interceptación, destrucción u ocultamiento de encomiendas y demás objetos postales para apropiarse de su contenido o interrumpir el curso normal de los mismos" (República Oriental de Uruguay, 1933)[130].

Es importante mencionar que el 16 de mayo de 2014, la Comisión de Constitución, Códigos, Legislación General y Administración de la República

[129] GAMBA, Jacopo.Op. Cit

[130] ROJAS PARRA, Jaime Hernán. Op. Cit. 227

Oriental de Uruguay presenta al presidente de la Asamblea General el proyecto de ley de delitos informáticos aprobada mediante nexos N° 17.616 (13 de enero de 2003, la cual consta de siete artículos, mediante los que se busca tipificar conductas punibles como las siguientes:

- Acceso no autorizado a todo o parte de un sistema informático.
- Daño a sistemas informáticos. Prisión de 6 a 36 meses.
- Estafa informática. Prisión de 6 a 48 meses.
- Suplantación de identidad mediante la utilización de tecnologías, para la cual hay penas de 18 a 96 meses de prisión.
- Tratamiento engañoso, abusivo o extorsivo de datos personales, 3 a 72 meses de prisión.
- Circunstancias de agravación punitiva[131].

SINOPSIS
En Uruguay, está presente la sección Delitos Informáticos del Departamento de Delitos Complejos, de la Dirección de Investigaciones de la Jefatura de Policía. Ley de Protección del Derecho de Autor y Derechos Conexos N° 17.616 (13 de enero de 2003) **Contenido** Normas que tutelan solamente la propiedad intelectual (software) **Técnica** Ley especial (se trata de buscar un aplicación amplia de las figuras clásicas introducidas por el código penal: hurto, estafa, daño)

Fuente: Adaptado de GAMBA[132]

[131] ROJAS PARRA, Jaime Hernán.Op. Cit.p. 227

[132] GAMBA, Jacopo.Op. Cit. p. 24

L.14 MÉXICO.

Mediante una reforma publicada el 6 de junio de 2007 se modifica el Código Penal Federal de México, con el objeto de penalizar las conductas relacionadas con la corrupción de menores e incapaces, pornografía infantil y prostitución sexual de menores, delitos en materia de derechos de autor, revelación de secretos y acceso ilícito a sistemas y equipos de informática.

El delito informático con mayor pena de prisión en México es "Transmitir, elaborar, reproducir, vender, arrendar, exponer o publicitar material que contenga grabaciones de actos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de 18 años" (Gobierno de México, 2007).

El 31 de enero del 2007 México fue invitado a adherirse al Convenio de Budapest, adhesión pendiente debido a que cuenta con el Estatuto de Observador ante el Consejo de Europa desde 1999, lo que le ha permitido tanto la realización de reformas constitucionales en telecomunicaciones, estrategias digitales nacionales, como ganar experiencia en el Comité Especializado en Seguridad de la Información del Consejo de Seguridad Nacional[133].

Con respecto al cibercrimen no existe una definición en la ley mexicana de los términos "cibercrimen" y "ciberseguridad"; sin embargo, el Código Penal Federal regula los comportamientos ilegales cometidos por medios electrónicos que

[133] ROJAS PARRA, Jaime Hernán.Op. Cit. 224

podrían identificarse como delitos informáticos mediante el uso de medios electrónicos para su comisión. A continuación según VELASCO[134] se relacionan algunos delitos tipificados el Código Penal Federal de México, a saber:

- Hackeo (es decir, acceso no autorizado). El artículo 211 bis del Código Penal Federal establece que quien, sin autorización, modifique, destruya o cause la pérdida de información contenida en sistemas o equipos informáticos protegidos por un mecanismo de seguridad, será sancionado con una pena de prisión de seis meses a dos años, por la autoridad pertinente, así como una multa de aproximadamente MN $ 8.004.00 a MN $ 24.012.00. La multa antes mencionada podría duplicarse en caso de que la información se use para beneficio propio o para beneficio de un tercero.
- Ataques de denegación de servicio. El Código Penal Federal no proporciona ninguna definición, o una definición similar, para este delito penal. Sin embargo, es una tipificación de delito informático.

- Suplantación de identidad. El Código Penal Federal no proporciona ninguna definición de phishing; sin embargo, dicho delito podría considerarse fraude. De acuerdo con el Artículo 386 del Código Penal Federal, una persona comete fraude cuando él/ella, con la intención de obtener una ganancia financiera, maneja la información a través del engaño, aprovecha los

[134] Velasco, Cristos. The Legal Framework on Cybercrime and Law Enforcement in Mexico,.Contribution to the Second WSIS Action Line C5 Facilitation Meeting, 207, p. 1-16 [Traducción en línea]

errores o engaña a una persona. En tal caso, la autoridad pertinente impondrá una pena de prisión de 3 a 12 años, así como una multa de aproximadamente MN $ 2.400.00 a MN $ 24.012.00, dependiendo del valor en cada caso.

- Infección de sistemas informáticos con malware (incluidos ransomware, spyware, gusanos, troyanos y virus). El Código Penal Federal no proporciona ninguna definición para este delito penal; sin embargo, este tipo de comportamiento es similar a la piratería. Las sanciones mencionadas son aplicables en este caso. En el evento de que el delito se cometa contra el Estado, la autoridad competente impondrá una pena de prisión de uno a cuatro años, así como una multa de aproximadamente MN $ 16.000.00 a MN $ 48.024.00.

- Posesión o uso de hardware, software u otras herramientas utilizadas para cometer delitos cibernéticos (por ejemplo, herramientas de piratería). El Código Penal Federal establece este delito penal como "piratería", que se describe anteriormente.

- Suplantación de identidad o fraude de identidad (por ejemplo, en relación con dispositivos de acceso). La Ley de Instituciones de Crédito establece que a una persona que produce, fabrica, reproduce, copia, imprime, vende, intercambia o altera cualquier tarjeta de crédito, tarjeta de débito, cheques o, en general, cualquier otro instrumento de pago, incluidos dispositivos

electrónicos, emitidos por instituciones de crédito, sin autorización del titular, la autoridad competente le impondrá una pena de prisión de tres a nueve años, así como una multa de aproximadamente MN $ 2.401.200.00 a MN $ 24.012.000.00. Además, el Código Penal Federal establece que una persona que, con o sin autorización, modifique, destruya o cause la pérdida de información contenida en los sistemas de las Instituciones de crédito o en los equipos informáticos protegidos por un mecanismo de seguridad, se le impondrá una pena de prisión de seis meses a cuatro años, por la autoridad competente, así como una multa de aproximadamente MN $ 8.004.00 a MN $ 24.012.00. Además, a una persona que sin autorización conozca o copie información en los sistemas informáticos o equipos de las instituciones de crédito protegidos por un mecanismo de seguridad se le impondrá una pena de prisión de tres meses, a dos años, así como una multa de aproximadamente MN $ 4.002.00 a MN $ 24.012.00.

- Hurto electrónico (por ejemplo, abuso de confianza por parte de un empleado actual o anterior, o infracción penal de derechos de autor). Como se mencionó, la Ley de Instituciones de Crédito establece que a cualquier persona que produzca, fabrique, reproduzca, copie, imprima, venda, negocie o altere, cualquier tarjeta de crédito, tarjeta de débito, cheque o, en general, cualquier otro instrumento de pago, incluidos dispositivos electrónicos, emitidos por entidades de crédito, sin autorización del titular, se le impondrá una pena de prisión de tres a nueve años, así como una

multa de aproximadamente MN $ 2.401.200.00 a MN $ 24.012.000.00. Las sanciones antes mencionadas pueden duplicarse si el delito es cometido por un asesor, funcionario, empleado o proveedor de servicios de cualquier institución de crédito.

- Cualquier otra actividad que afecte o amenace negativamente la seguridad, confidencialidad, integridad o disponibilidad de cualquier sistema de TI, infraestructura, red de comunicaciones, dispositivo o datos de espionaje; conspiración; delitos contra los medios de comunicación; aprovechamiento de las comunicaciones; actos de corrupción; extorsión; y el lavado de dinero podrían considerarse como amenazas a la seguridad, confidencialidad, integridad o disponibilidad de cualquier sistema de TI, infraestructura, red de comunicaciones, dispositivo o datos[135].

L.15 CHILE

Chile fue invitado oficialmente por el Consejo de Europa a adherirse al Convenio de Budapest desde 2009, pero hasta ahora, Chile no ha completado el procedimiento de adhesión como se describe en los artículos 27 y 38 del Convenio de Budapest. La aplicación del derecho penal se establece en el artículo 5, que se basa en el principio de territorialidad, así como en el artículo 6 del Código Penal de

[135] Velasco, Cristos. The Legal Framework on Cybercrime and Law Enforcement in Mexico. Contribution to the Second WSIS Action Line C5 Facilitation Meeting, 2007, pp. 1-16 [Traducción en línea]

Chile, que establece los límites del principio de extraterritorialidad del derecho penal[136].

Los delitos relacionados con el uso de Información y sistemas Informáticos que son sancionados y castigados en Chile son los siguientes:

- Destrucción o Inhabilitación de los sistemas de procesamiento de Información o para prevenir o modificar su funcionamiento (Art. 1o. Ley 19.223 del 7 de Junio de 1993)
- Tomar posesión, usar o conocer indebidamente la información contenida en un sistema de procesamiento de información o para interceptar, interferir o acceder al sistema de información (Art. 2o. Ley 19.223 del 7 de Junio de 1993)
- Alterar, dañar o destruir maliciosamente los datos contenidos en un sistema de procesamiento de datos (Art. 3o. Ley 19.223 del 7 de junio de 1993)
- Revelar o difundir maliciosamente los datos contenidos en un sistema de información (Art. 4o. Ley 19.223 del 7 de junio de 1993)
- Realizar actos sexuales con menores (Art. 366, 366 bis y 366 ter Código Penal)
- Producción de contenido pornográfico sea cual sea su soporte o medio donde para su creación o producción se utilizaron menores de edad (Art. 366 Código Penal)
- Promoción y facilitación de la prostitución de menores (Art. 367 Código Penal)
- Intercepción de telecomunicaciones o grabación de individuos sospechosos o de una organización criminal, como fotografía, película u otros medios para reproducir imágenes que ayuden a aclarar crímenes que involucran pornografía infantil, así como el uso de agentes encubiertos a solicitud del Fiscal Público (Art. 369 ter Código Penal)
- Comercializar, importar, exportar, distribuir, difundir o exhibir material pornográfico en cualquier medio o por medio de sistemas de telecomunicaciones cuya producción se haya utilizado para menores (Art. 374 bis y 374 ter Código Penal)
- Capturar, interceptar, grabar o reproducir conversaciones o comunicaciones privadas sin permiso de la persona afectada, así como robar, fotografiar, fotocopiar o reproducir documentos o instrumentos privados en locales privados o lugares que no son accesibles al público y difundir comunicaciones, documentos , instrumentos, imágenes y hechos (Art. 161-A Código Penal).

Fuente: Adaptado de ZÚÑIGA & LONDOÑO[137]

[136] ZÚÑIGA, Rodrigo y LONDOÑO, Fernando. Cybercrime and jurisdiction in Chile. En: Cybercrime Jurisdiction: A Global Survey. 2006, p. 141-155

[137] ZÚÑIGA, Rodrigo y LONDOÑO, Fernando.Op. Cit.

Chile cuenta con Instituciones especializadas, tales como: Los poderes del Ministerio Público para investigar los actos que constituyen delitos se establecen en los artículos 80-A y 80-B de la Constitución chilena. El Ministerio Público es el único responsable de llevar a cabo las investigaciones de los hechos que constituyen delitos, incluido el delito cibernético y de ejercer el enjuiciamiento público penal, según lo dispuesto en su Ley Orgánica Constitucional.

La Policía de Investigaciones de Chile tiene una unidad de Investigación especializada en ciberdelincuencia llamada "Brigada Metropolitana de Investigación de Delitos Cibernéticos" desde octubre de 2000, cuyas funciones principales son detectar e investigar conductas ilegales en Internet, proporcionar evidencia a los tribunales y fiscales y proporcionar capacitación y formación en investigación, en delitos informáticos. La Brigada Metropolitana de Investigación de Delitos Cibernéticos se compone de tres áreas: (i) Delitos en Internet contra los niños: (ii) delitos informáticos: y (iii) Informática forense[138].

Chile cuenta con un Centro de Respuesta a Incidentes de Computación y Seguridad conocido como CSIRT-CL, patrocinado por el Ministerio del Interior y Seguridad Pública, cuya misión principal incluye: (i) proporcionar información y asistencia a la Conectividad de Red del Estado y, en general, el ciberespacio del gobierno; (ii) administrar un sistema de cooperación nacional e Internacional en materia de ciberseguridad, a fin de reducir el riesgo y articular la respuesta cuando

[138] ZÚÑIGA, Rodrigo y LONDOÑO, Fernando.Op. Cit.

los delitos se materialicen realmente; (iii) promover buenas prácticas en ciberseguridad dentro de la administración del gobierno; (iv) promover la protección de las infraestructuras críticas de información y los recursos clave del país; (v) promover el fortalecimiento del marco legal en relación con la informática y el delito cibernético y (vi) promover la conciencia sobre ciberseguridad[139].

Una vez se ha analizado desde la perspectiva del derecho comparado, la legislación sobre el delito informático o ciberdelito, se puede concluir que existe diversidad de criterios, no unificados ni tipificados, que permitan establecer un estándar internacional, especialmente cuando se trata de analizar la legislación existente en un país como Colombia, frente a otros de la comunidad internacional. Cada uno de los países tiene su respectivo marco jurídico dependiendo de la influencia histórica de las tendencias europeas, inglesa, francesa, española y americana. Para el caso colombiano, existen muchas diferencias frente los países analizados, sin embargo, con respecto a España, dada la influencia en este campo, existen muchas similitudes en torno a la tipificación de la transferencia no consentida de activos, pues en otros países simplemente se considera como estafa, apropiación ilícita, hurto, entre otras acepciones al concepto planteado en esta investigación.

[139] ZÚÑIGA, Rodrigo y LONDOÑO, Fernando.Op. Cit.

L.16 ECUADOR

Con respecto al Ecuador, la legislación existente sobre el ciberdelito está contemplado en el Código Orgánico Integral Penal 2014, en la sección novena cuando en su artículo 190 reza:

> Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes[140.]

[140] Código Orgánico Integral Penal, del Ecuador 2014 [En línea] Recuperado de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf [10-11-19]

De acuerdo al contexto del artículo anterior, existe cierta similitud con el código penal colombiano respecto a la consideración de transferencia no consentida de activos. Más adelante, en la sección tercera sobre delitos contra la seguridad de los activos de los sistemas de información y comunicación, el artículo 231 del mencionado Código Orgánico Integral Penal del Ecuador, señala taxativamente la transferencia electrónica de activo patrimonial al igual que la alteración o manipulación del funcionamiento informático o manejo ilícito de datos con fines de transferencia apropiación no consentida de activo patrimonial, la cual es sancionada con pena privativa de libertad de tres a cinco años. También el artículo 232 contempla el ataque a la integridad de sistemas informáticos como un delito con pena privativa de libertad de tres a cinco años.

Analizada la legislación del Ecuador en el marco del ciberdelito y su comparación con el caso colombiano, existe similitud frente al derecho penal y su aplicación punitiva en cuanto al delito informático, especialmente en lo concerniente a la transferencia no consentida de activos, contemplada en el artículo 269J del Código Penal de Colombia.

Con respecto a las legislaciones de los países de Francia, Italia, Australia, Canadá, Reino Unido, Estados Unidos, Argentina, Brasil, Perú, Uruguay, México, Chile, en torno al ciberdelito y su comparación con el caso colombiano, no hay similitudes frente al derecho penal y su aplicación punitiva en cuanto al delito

informático, ni tampoco con referencia a la transferencia no consentida de activos, contemplada en el Código Penal de Colombia.

M. TIPOLOGÍA DE DELITOS SEGÚN LA LEGISLACIÓN INTERNACIONAL

Después de analizar dentro del marco del derecho comparado con respecto al ciberdelito, a manera de conclusión las nociones de delincuencia informática, delincuencia relacionada con la informática, delincuencia de alta tecnología y de delincuencia cibernética tienen el mismo significado en cuanto se refieran a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles[141].

En síntesis, los principales delitos tratados por la legislación existente a nivel internacional se pueden representar de manera resumida en la siguiente tabla.

Tabla 3. Tipología de delitos según la legislación internacional

– Delitos contra la propiedad intelectual: delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines; – Delitos contra la intimidad: recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales; – Delitos relativos al contenido: difusión, especialmente por internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia; – Delitos económicos, acceso no autorizado: muchos países han aprobado leyes que

[141] WINMILL, B Lynn, METCALF, David L y BAND, Michael E Cybercrime: Issues and challenges in the United States. [Traducción en línea] En: Digital Evidence Elec. Signature L. Rev. 2010. vol. 7, p. 19

	abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático, la distribución de virus, el espionaje informático, la falsificación y el fraude informáticos)

Fuente: Adaptado de GAMBA[142]

N. LA CONVENCIÓN DE BUDAPEST, PROPÓSITOS Y SITUACIÓN ACTUAL

La Convención sobre Cibercrimen del Consejo de Europa (CETS No.185), conocida como la Convención de Budapest, es el único instrumento internacional vinculante sobre este tema. Sirve como una guía para cualquier país que desarrolle una legislación nacional integral contra el Cibercrimen y como un marco para la Cooperación Internacional entre los Estados que hacen parte de este tratado. La Convención de Budapest se complementa con un Protocolo sobre Xenofobia y Racismo cometido a través de sistemas informáticos.

La Convención sobre Cibercrimen del Consejo de Europa se firmó en Budapest en noviembre de 2001. Quince años después, sigue siendo el acuerdo internacional más relevante sobre cibercrimen y evidencia electrónica. La membresía sigue creciendo, mientras que la calidad de la implementación y el nivel de cooperación entre las Partes siguen mejorando, y el tratado en sí mismo está evolucionando para enfrentar nuevos desafíos. La fórmula del éxito es un "triángulo dinámico". La Convención de Budapest se complementa con un

[142] GAMBA, Jacopo.Op. Cit.

mecanismo de seguimiento eficaz y con programas de creación de capacidad, que se retroalimentan en el Comité y contribuyen a la evolución de la Convención[143].

El cibercrimen ha existido por más de 40 años. El Consejo de Europa había tratado este tema desde la perspectiva del derecho penal, desde mediados de los años ochenta en adelante. Para 2001, la terna se había vuelto lo suficientemente importante como para justificar un tratado internacional vinculante. Negociada por los Estados miembros del Consejo de Europa, junto con Canadá, Japón, Sudáfrica y los Estados Unidos de América, la Convención sobre Ciberdelincuencia se abrió a la firma en Budapest, Hungría, en noviembre de 2001.

Desde entonces, las tecnologías de la información y la comunicación (TIC) han transformado las sociedades en todo el mundo. También los han hecho altamente vulnerables a riesgos de seguridad como el cibercrimen. Si bien se reconoce la necesidad de fortalecer la seguridad, la confianza en las TIC y reforzar el estado de derecho y la protección de los derechos humanos en el ciberespacio, todas las cosas "cibernéticas" se han vuelto demasiado importantes. A medida que se refieren a los derechos fundamentales de las personas, así como a los intereses nacionales (de seguridad) de los Estados, es cada vez más difícil llegar a un consenso internacional sobre soluciones comunes[144].

[143] DE HERT, Paul, PARLAR, Cihan y SAJFERT, Juraj The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. 2018. vol. 34, no. 2, p. 327-336 [Traducción en línea]

[144] Ibid.

Para superar este dilema, el enfoque más sensato es enfocarse en estándares comunes que ya están vigentes y en funcionamiento, como la Convención de Budapest sobre Cibercrimen, y en enfoques sobre los cuales existe un amplio acuerdo, en particular, el desarrollo de capacidades.

La Convención de Budapest es un tratado de justicia penal que brinda a los Estados instrumentos en torno a : (i) la penalización de una lista de ataques contra y por medio de computadoras; (ii) herramientas de derecho procesal para hacer que la investigación del delito cibernético y la obtención de evidencia electrónica en relación con cualquier delito sea más efectiva y esté sujeta a las salvaguardas del estado de derecho; y (iii) cooperación policial y judicial internacional en cibercrirnen y evidencia electrónica[145].

Está abierto a la adhesión de cualquier Estado preparado para ¡implementarlo y cooperar. Para noviembre de 2016, que también marcó el 15 aniversario de la Convención, 50 Estados eran Partes (países europeos, así como Australia, Canadá, República Dominicana, Israel, Japón, Mauricio, Panamá, Sri Lanka y los Estados Unidos). Otros 17 de todas las regiones del mundo lo habían firmado o habían sido invitados a acceder.

Estos Estados que actualmente ascienden a 67, junto con diez organizaciones internacionales (como la Secretaría de la Commonwealth, la Unión Europea, INTERPOL, la Unión Internacional de Telecomunicaciones, la

[145] DE HERT, Paul, PARLAR, Cihan y SAJFERT. Op. Cit.

Organización de los Estados Americanos, la Oficina de las Naciones Unidas contra la Droga y el Delito y otros), participan corno miembros u observadores en el Comité de la Convención de Delitos Cibernéticos. Este Comité evalúa la implementación de la Convención por las Partes y mantiene la Convención actualizada. Los esfuerzos actuales se centran en soluciones relacionadas con el acceso de la policía a la evidencia electrónica en servidores en la nube.

El valor del desarrollo de capacidades en relación con el cibercrimen y la seguridad no es un descubrimiento nuevo. Las llamadas internacionales para asistencia técnica para reforzar las capacidades de justicia penal en cibercrimen se han hecho durante décadas. Luego de la adopción de la Convención de Budapest sobre Cibercrimen en 2001, el Consejo de Europa comenzó a ayudar a los países en la implementación de este tratado, primero dentro de Europa, y desde 2006, también en otras regiones del mundo, a menudo en cooperación con la Unión Europea.

Sin embargo, en febrero de 2013 se llevó el asunto a otro nivel. El Grupo Intergubernamental de Expertos de las Naciones Unidas en Delito Cibernético y la Unión Europea en su Estrategia de Ciberseguridad declararon la necesidad de un acuerdo amplio sobre creación de capacidad.

En octubre de 2013, fue el foco de la Conferencia Global del Ciberespacio en Seúl, Corea. Sobre la base de este impulso, la Unión Europea y el Consejo de Europa siguieron de inmediato y en la misma semana firmaron su acuerdo sobre

el proyecto conjunto sobre “Acción Global contra el Cibercrimen” (GLACY), mientras que al mismo tiempo, el Consejo de Europa decidió establecer una Oficina del Programa de Delitos Cibernéticos (C-PROC) para la creación de capacidad mundial en Bucarest, Rumania. La creación, en la posterior Conferencia Mundial del Ciberespacio (Países Bajos, abril de 2015), del Foro Global sobre Experiencia Cibernética fue una consecuencia lógica adicional[146].

Para agosto de 2016, C-PROC gestionó una serie de proyectos, incluidos varios conjuntos con la Unión Europea, que cubren la región de la Asociación Oriental (Armenia, Azerbaiyán, Bielorrusia, Georgia, Moldavia y Ucrania) o el sudeste de Europa y Turquía (el proyecto “PROCEEDS” apunta a los ingresos del crimen en línea).

Con un alcance geográfico más amplio, el proyecto “Acción Global contra el Cibercrimen” (GLACY) ayuda a Marruecos, Filipinas, Senegal, Sudáfrica, Sri Lanka y Tonga. Estos son países prioritarios dado su compromiso político para implementar la Convención de Budapest. Con GLACY finalizando, en octubre de 2016, varios de estos países podrán compartir su experiencia dentro de sus respectivas regiones sirviendo como centros bajo el nuevo proyecto conjunto UE-CoE “Acción Global contra el Cibercrimen Extendido” (GLACY +), que se extiende desde 2016 hasta 2020 (Stancu, 2016).

[146] DE HERT, Paul, PARLAR, Cihan y SAJFERT. Op. Cit.

La experiencia de los últimos años ha demostrado que el desarrollo de capacidades es una forma efectiva de ayudar a las sociedades a enfrentar el desafío del delito cibernético. En términos generales, el compromiso político, la referencia a estándares internacionales comunes y la participación continua en revisiones internacionales puede convertirse en una estrategia para combatir el ciberdelito.

Para el Consejo de Europa, la Convención de Budapest, el Comité de la Convención sobre el delito cibernético y el desarrollo de capacidades de C-PROC forman un "triángulo dinámico": los programas de creación de capacidad apoyan la implementación de la Convención de Budapest, así corno las recomendaciones del Comité de la Convención sobre el delito cibernético; y, al mismo tiempo, la experiencia de los programas de creación de capacidad se retroalimenta al Comité y la evolución de la Convención. La participación a largo plazo de los "países del proyecto" en el Comité de la Convención de Delitos Cibernéticos ayuda a mantener el proceso más allá del ciclo de vida de los proyectos individuales[147]

El objetivo de esta convención internacional es recurrir a la colaboración internacional entre países, de manera que se establezca que una conducta lesiva sea delito en cada jurisdicción. Así, no obstante se mantengan y se respeten las legislaciones locales, los Estados deben definir delitos informáticos basados en un

[147] STANCU, Adriana Iuliana Evolution Of The International Regulations Regarding Cybercrime. En: Public Administration Regional Studies. 2016. vol. 18, no. 2, p. 72-79. [Traducción en línea]

modelo común. La Convención sobre cibercrimen, firmada en Budapest en 2001, entró en vigencia el 1º. de julio de 2004 y en su redacción participaron los 41 países miembros del Consejo de Europa, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica[148].

El enfoque subyacente de la Convención es reconocer la necesidad de armonizar las legislaciones nacionales. La Convención introduce elementos de derecho sustancial penal, junto a previsiones de derecho procesal, principios para la coordinación internacional, extradición y medidas provisionales. En otras palabras, trata del argumento de manera completa y exhaustiva, dictando normas y sugiriendo reglas de organización entre diferentes instituciones policiales.

En el sector penal, la armonización se ha logrado en materia de tratados de extradición y de existencia legal mutua que permite a los gobiernos compartir información y evidencia. Existe, por ejemplo, el requerimiento de la llamada dualidad criminal (el acto que se investiga debe ser un crimen en ambas legislaciones; los gobiernos deben tener la capacidad de aplicar las leyes).

Los delitos cibernéticos frecuentemente tienen implicaciones de seguridad nacional y de procedimientos de inteligencia, lo cual complica la colaboración. Por lo tanto, resultará útil establecer redes de confianza entre las agencias encargadas

[148] LUONG, Hai Thanh. Cybercrime in Legislative Perspectives: A Comparative Analysis between the Budapest Convention and Vietnam Regulations. [Traducción en línea] En: International Journal of Advanced Research in Computer Science. 2019. vol. 10, no. 3, p. 1

de combatir el crimen cibernético en los diversos países para crear una red de investigación y punición que no sea obstaculizada con las fronteras[149].

[149] GAMBA, Jacopo.Op. Cit.p.27

CAPITULO II. EL DELITO INFORMÁTICO EN EL MARCO JURÍDICO DE COLOMBIA

A. Antecedentes investigativos para el caso colombiano

La literatura es abundante sobre un tema tan trascendente y de mucha actualidad, que merece ser analizada desde la perspectiva de las necesidades del país y su inserción en el mundo globalizado, donde las TIC han permeado las actividades de toda la sociedad y por lo tanto, los riesgos son más latentes y exige del legislador medidas para prevenir el delito y establecer castigos del código penal que estén orientados a minimizar su comisión.

En primera instancia, se cuenta con el análisis realizado por GRISALES P[150]. (2013b), en cuyo documento justifica la necesidad de abordar el tema, debido al incremento del delito informático no sólo a nivel colombiano sino en el contexto mundial, donde la transferencia no consentida activos por medios informáticos está afectando al país, tanto a las personas naturales como jurídicas, en detrimento patrimonial, debido a sus bienes económicos y ante todo la información privada a la que acceden los delincuentes cibernéticos. En ese documento, también se analiza el bien jurídico protegido según el derecho penal, la caracterización de los diferentes delitos informáticos, la recitación de la conducta,

[150] GRISALES P., G. Análisis dogmático de las conductas de hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j) ley 1273 de 2009 Maestría en Derecho Penal. Medellín: Universidad EAFIT. Escuela de Derecho, 2013.

los sujetos activo y pasivo, la acción o conducta, el objeto material, entre otros temas.

En el tema del delito informático su tratamiento para el caso colombiano, está la publicación del libro de SUÁREZ S[151]., denominado manual de delito informático en Colombia, análisis dogmático de la ley 1273 de 2009, en cuya obra se analizan los aspectos generales de la delincuencia informática, las normativas internacionales sobre dichos delitos, el tratamiento de la criminalidad informática, la caracterización del delito informático a nivel global y en Colombia, la regulación del delito informático en el derecho penal colombiano, el bien jurídico de los delitos contra la información y los datos, su clasificación, la parte objetiva y subjetiva de los tipos penales contra los datos y la información, el daño informático, el uso de software malicioso, la violación de los datos personales, la suplantación a través de la web, el hurto por medios informáticos semejantes y un capítulo especial sobre la transferencia no consentida de activos y circunstancias modificadoras de las penas de los delitos informáticos.

Otra obra del mismo autor SUÁREZ S[152]., corresponde al tratado sobre la estafa informática, una obra de la biblioteca de tesis doctorales donde se analiza la criminalidad informática, la caracterización del delito informático, la normativa internacional sobre este tipo de delitos, la regulación del delito informático en el

[151] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit.

[152] SUÁREZ S., A. La Estafa Informática. 2015. Op. Cit.

derecho penal español, evolución jurisprudencial y doctrinal de las derogaciones informáticas en España, la regulación del delito informático el derecho penal colombiano, la estafa informática, el bien jurídico, el injusto típico del estafa informática, la manipulación de tarjetas magnéticas, todo esos temas dentro del marco del derecho comparado entre España y Colombia. Otro gran referente a tener en cuenta para realizar un análisis a profundidad sobre la estafa informática, relacionada con el tema objeto de este estudio monográfico.

A nivel de artículos de revistas especializadas, se encuentra el realizado por R. POSADA M[153]., denominado: El delito de transferencia no consentida de activos. En este artículo, se analiza la transferencia no consentida de activos mediante el uso de software destinado a los fraudes inherentes a los delitos informáticos y la cibercriminalidad. Argumenta que los delitos informáticos de naturaleza económica se han incrementado en la medida del mayor uso de las TIC, lo cual constituye un reto para el Estado y las jurisdicciones de diferentes países, por cuanto existe mucha precariedad dogmática para castigar el comportamiento delictivo informático, lo que afecta el patrimonio económico de las organizaciones y personas civiles, especialmente en el campo financiero.

Dentro de los delitos informáticos para el caso colombiano, está el artículo realizado por MANJARRÉS y JIMENEZ T[154]., en el que se argumenta que debido

[153] POSADA M. Op. Cit.

[154] MANJARRÉS, B., I. y JIMENEZ T., F. Caracterización de los delitos informáticos en Colombia. En: Revista Pensamiento Americano. 2014. vol. 5, no. 9, p. 71-81

a los avances tecnológicos en la sociedad cada vez más globalizada, los cuales permiten mayor almacenamiento, transferencia y gestión de la información, también han generado un aumento inusitado de transacciones comerciales, comercio electrónico, comunicaciones online, incorporación de las energías en procesos industriales, de investigación, seguridad y transferencias electrónicas entidades financieras, generando altos riesgos para las empresas, las personas y el Estado en general, por lo cual los comportamientos ilícitos agrupados bajo el concepto de “delitos informáticos”, merecen un estudio interdisciplinario desde la academia, a fin de generar mayor conciencia en el manejo de la información, generándose un gran desafío para las autoridades y la jurisprudencia para su castigo y garantía de seguridad.

Continuando con la exploración y análisis de los referentes más importantes sobre el delito informático para el caso colombiano, está el artículo realizado por J. SALAZAR J[155]., denominado: situación normativa de la sociedad de la información en Colombia. En este artículo se hace un análisis sobre los grandes temas que afectan al país dada su disminución de la brecha tecnológica entre los países y el crecimiento en el uso de las TIC, especialmente en el campo del comercio electrónico, las firmas digitales las entidades de certificación y el crecimiento de los delitos informáticos cometidos a través de las redes y el ordenador. Se compara los esfuerzos normativos realizados por organismos internacionales en

[155] SALAZAR, Juan Fernando. Situación normativa de la Sociedad de la Información en Colombia. En: Criterio Jurídico. 2011. vol. 9, no. 1, p. 89-103

este tema y los avances regulatorios en el comercio electrónico a través de la ley 527 de 1999 y la ley 1273 de 2009 denominada ley de delitos informáticos, la cual constituye una norma disuasoria contra la criminalidad electrónica, que si bien busca aumentar la confianza del público en uso de los medios electrónicos, la aplicación penal a los delitos cometidos, dejan vacíos jurídicos por qué estos se cometen muchas veces fuera de la jurisdicción territorial y no dejan rastro sobre las acciones punibles.

En este mismo sentido, está el artículo de DIAZ G.[156], denominado aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la ley de delitos informáticos. En el documento se resaltan los avances que ha tenido Colombia en este campo y soporta el autor el trabajo realizado desde su ejercicio como juez de la República en Rovira, en términos de concientizar a la judicatura y a los jurisconsultos el tema del delito informático. A partir de la convención de Budapest, un referente para implementar un proceso de legislación sustantiva y disposiciones procesales, especialmente en materia de cooperación internacional y asistencia mutua, al tenor de la propia aplicación de la convención. La vigencia de la ley informática en la definición del bien jurídico tutelado en el contexto jurídico, la tipificación de las conductas debido a la proliferación de fraudes y delitos conexos contra el patrimonio y la información personal, es un avance significativo para la prevención y protección no sólo del

[156] DIAZ G., A. Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos. 2010

Estado, sino también de las empresas, las organizaciones y la ciudadanía en general.

B. Antecedentes Normatividad Nacional datos y delitos informáticos

Como antecedentes sobre normativa nacional en materia de medios informáticos, protección de datos y delito informático, cabe mencionar los esfuerzos realizados por Colombia en su legislación de manera cronológica, tal como se observa en la reciente tabla, iniciando con la ley de comercio electrónico y la ley en la cual se expide el código penal.

Tabla 4. Antecedentes de la Normatividad colombiana sobre datos y delitos informáticos

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 527 de 1999 - COMERCIO ELECTRÓNICO	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
Ley 599 de 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."

Fuente: Tomado de CONPES[157]

[157] Conpes 3701 de 2011 Op. Cit.p.10

Otro referente que abordó el tema relacionado con el delito informático fundamentalmente en lo que respecta al daño en soportes lógicos, bases de datos, herramientas, equipos, instalaciones y materias primas para el uso adecuado de un sistema de información, fue el tipo penal de sabotaje, estableciendo que:

> "El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de dieciséis (16) a ciento ocho (108) meses y multa de seis punto sesenta y seis (6.66) a treinta (30) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor[158].
>
> Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspensión o cesación colectiva del trabajo, la pena se aumentará hasta en una tercera parte (penas aumentadas por el artículo 14 de la Ley 890 de 2004, a partir del 1o. de enero de 2005).

La normatividad y los avances de la legislación colombiana en materia de reformas al código penal, la racionalización de trámites y procedimientos administrativos, medidas de transparencia y eficiencia, definición de conceptos sobre la Sociedad de la información y las TIC, así como la regulación en materia de comunicaciones, se muestra en la siguiente tabla.

[158] Ley 599 de 2000, artículo 199

Tabla 5. Normatividad Nacional en la materia

LEY / RESOLUCIÓN CIRCULAR	TEMA
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública – Secop.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones –TIC y se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Fuente: Tomado de CONPES[159]

Los anteriores referentes nacionales sobre la protección de la seguridad informática y la lucha de los delitos informáticos que se vienen cometiendo a nivel nacional e internacional a través del Internet, redes sociales y los sistemas informáticos, que afectan la seguridad del Estado, las organizaciones, la sociedad civil en general, merece las consideraciones analíticas e interpretativas para abordar un tema de tanta actualidad desde el derecho penal en torno a la transferencia no consentida de activos por medios informáticos, especialmente en el sistema financiero colombiano.

[159] Ibid.p.11

C. La Legislación Colombiana en el marco del Código Penal

Como ya se ha comentado, la globalización y su manifestación en todos sus niveles de la sociedad, junto con el desarrollo y masificación de las TIC, de manera paralela han proliferado una serie de delitos que se cometen a través de sistemas informáticos en Internet. Las particularidades y tipificación de estos delitos, exigen un tratamiento transnacional, según convenios internacionales, como referentes para realizar ajustes normativos a la legislación de cada uno de los países de la comunidad internacional, para adoptar medidas globales de cooperación y combatir el ciberdelito de forma integral a través de la "armonización del derecho sustantivo, así como en el ámbito procesal, que redunde definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales"[160].

Al respecto, Colombia no tiene una legislación independiente o específica para castigar el delito cibernético. El marco legal para castigar los delitos cometidos mediante el uso de tecnología y sistemas de información está contenido principalmente en el Código Penal y otras leyes a nivel nacional, como es el caso de la Ley 1273, de 5 de enero de 2009, que modifica el Código Penal Colombiano, con el objeto de crear un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos", además de preservar integralmente

[160] DÍAZ GÓMEZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR. 2010, no. 8, p. 169-203

los sistemas que utilicen las tecnologías de la información y las comunicaciones. El Congreso de Colombia decreta la adición al Código Penal del título VII bis, “De la protección de la información y de los datos”, el cual se compone únicamente de dos capítulos, el primero versa sobre los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos en los sistemas informáticos y, el segundo relacionado con los atentados informáticos y otras infracciones. Esta ley, busca sancionar la Comisión de diferentes tipologías de delitos que con mayor frecuencia se cometen en Colombia. Según MANJARRÉS y JIMENEZ T[161]., presenta una clasificación de los delitos informáticos en Colombia, entre los cuales están aquellos que:

- Afectan el patrimonio económico: banca virtual, phishing, key logers, falsas páginas, venta a través de portales de compra y venta, falsos premios.

- Buscan el abuso de menores: comercializan videos, fotografía, audio, texto, falsas agencias, salas de chat.

- Afectan la propiedad intelectual: descargas de programas y comercialización de obras sin pagar derechos de autor.

- Afectan la información como bien jurídico: como por ejemplo cuando algunos empleados usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia, teniendo como base el desarrollo que han tenido. Apropiación ilícita de información privilegiada.

[161] MANJARRÉS, B., I. y JIMENEZ T., F.Op. Cit. p. 77

MANJARRÉS y JIMENEZ T.[162] sostienen que la Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones.

A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos[163].

D. Ley 1273 de 2009, ley fundamental

La ley fundamental o ley 1273 de 2009, consagra dos capítulos como adición al Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos". El primer capítulo, de los atentados contra la confidencialidad, integridad y disponibilidad de los datos en los sistemas informáticos contiene siete artículos, los cuales se detallan en la siguiente tabla.

[162] MANJARRÉS, B., I. y JIMENEZ T., F.Op. Cit.

[163] Ibid.

Tabla 6. Capitulo I. De los atentados contra la confidencialidad, integridad y la disponibilidad de los datos en los sistemas informáticos (Ley 1273 de 2009)

Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación*. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: *Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Fuente: Tomado de Diario Oficial[164].

De la tabla anterior se deduce que los enunciados, alcance y características de los diferentes delitos informáticos relacionados con los datos y los sistemas informáticos, muestran que la penalización en este tipo de delitos, se encuentra entre las más desarrolladas de América Latina, tomando como marco la Directiva de protección de datos de la UE (95/46 / CE), que desde entonces ha sido reemplazada por el Reglamento general de protección de datos de la UE (2016 / 679) y, en ese sentido, no considera las tendencias existentes, como el interés

[164] Ley 1273 de 2009 (enero 5) Diario Oficial No. 47.223 de 5 de enero de 2009

legítimo y otras alternativas para consentir el procesamiento legal de datos personales.

Sobre la legislación vigente que protege la recopilación, almacenamiento y uso de los datos personales, merece especial atención mencionar el marco jurídico sobre el particular, que es bastante amplio, como se relaciona a continuación:

- El artículo 15 de la Constitución, que establece el derecho fundamental a habeas data o privacidad de datos;
- La Ley 1266/2008, que es la ley estatutaria que regula el Artículo 15 de la Constitución con respecto a los derechos de privacidad de datos de individuos y entidades legales exclusivamente en lo que respecta a los informes de historial crediticio y la consulta con agencias de crédito;
- Ley 1273/2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- La Ley 1581 /2012, que es la ley general de protección de datos estatutaria más completa de Colombia y regula todo el procesamiento de datos personales;
- Decreto 1377/2013, que es la regulación secundaria más extensa y completa de la Ley 1581/2012;
- Decreto 886/2014, que regula el Registro Nacional de Bases de Datos administrado por la Autoridad de Protección de Datos;
- Decreto 1759/2016, que extendió el plazo para que los controladores de datos colombianos que son entidades legales se registren en el Registro Nacional de Bases de Datos hasta el 30 de junio de 2017;
-

- Decreto 1115/2017, que extendió la fecha límite para que los controladores de datos colombianos que son entidades legales se registren en el Registro Nacional de Bases de Datos hasta el 31 de enero de 2018; y
- Varias circulares y directrices de la Superintendencia de Industria y Comercio relativas a:

    - la implementación del principio de rendición de cuentas;
    - declaraciones de conformidad para transferencias transfronterizas de datos personales; o normas de adecuación para las transferencias transfronterizas de datos personales; o sistemas de notificación para CCTV; y o la contratación de servicios en la nube.

Por otra parte, frente a este marco jurídico sobre protección de datos, es necesario establecer su alcance y jurisdicción, el cual está centrado en las personas físicas y jurídicas cuya información financiera o crediticia se almacena en bases de datos en poder de entidades privadas o públicas, por lo tanto, hacen parte del ámbito de la Ley 1266/2008. Las personas que residen o cuyos datos personales se almacenan o procesan en cualquier base de datos en Colombia caen dentro del alcance de la Ley[165].

En cuanto a la tipología de datos dentro del alcance de la legislación vigente, está relacionada con datos sobre el historial crediticio de un individuo, el cual cae dentro del alcance de la Ley 1266/2008 y todos los datos personales que identifican o son susceptibles de identificar a un individuo caen dentro del alcance de la Ley 1581 /2012.

[165] Ley 1581 de 2012.

En cuanto a la información sobre la propiedad de los datos registrados y su disponibilidad pública, según la Ley 1581/2012, los "sujetos de los datos", se definen como los propietarios de los datos personales. Por lo tanto, significa que los controladores de datos (que son los custodios, pero nunca los propietarios de los datos personales), son responsables de salvaguardar dicha información dado que está disponible públicamente en el Registro Nacional de Base de Datos. La única información incluida en el registro que no está disponible públicamente se refiere a:

- medidas de seguridad;
- quejas presentadas por los interesados; y
- detalles de incidentes de seguridad (es decir, violaciones de datos).

En cuanto al organismo responsable de hacer cumplir la legislación de protección de datos, corresponde a la Superintendencia de Industria y Comercio, como la autoridad de protección de datos más importante para la aplicación de:

- Ley 1266/2008 (una ley estatutaria que regula el Artículo 15 de la Constitución con respecto a los derechos de privacidad de datos de individuos y entidades legales exclusivamente en lo que respecta a la presentación de informes de historial crediticio y consultas con agencias de crédito); y,
- Ley 1581 /2012 (la ley general de protección de datos más completa de Colombia, que rige todo el procesamiento de datos personales).

Por otra parte, al analizar el segundo capítulo de la Ley 1273 de 2009, el cual está relacionado con los atentados informáticos y otras infracciones, éste sólo contiene dos artículos, el primero referente al hurto por medios informáticos y semejantes y el segundo, tema central de esta investigación, la transferencia no consentida de activos. La siguiente tabla muestra la definición, contesto, alcance y sanciones establecidas según el código penal para este tipo de delitos.

Tabla 7. Capitulo II. De los atentados informáticos y otras infracciones (Ley 1273 de 2009)

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. **Artículo 269J:** *Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad Artículo 2o. Adiciónese al artículo 58 del Código Penal con un numeral 17, así: Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: (...) 17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3o. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen:

(...) 6. De los delitos contenidos en el título VII Bis. (De la Protección de la información y de los datos).

Artículo 4o. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

Fuente: Diario Oficial No. 47.223 de 5 de enero de 2009[166]

Los anteriores delitos tipificados en la ley en cuestión, especialmente la transferencia no consentida de activos, hacen parte del propósito fundamental de esta investigación monográfica. Si bien el legislador colombiano ha establecido la comisión de este tipo de delito de manera general, en la práctica los ciberdelitos son cada vez más sofisticados por el avance tecnológico, lo cual brinda oportunidad para cometer estafa, suplantación de identidad, transacciones financieras no consentidas, acceso mediante claves de tarjetas de débito y crédito, entre otros.

De la exploración y análisis de este delito sobre transferencia no consentida de activos, se encontró que en la mayoría de países no figura bajo este concepto, a excepción de España que según SUÁREZ S[167], en nota de pie de página, trascribe:

[166] Ley 1273 de 2009 (enero 5) Diario Oficial No. 47.223 de 5 de enero de 2009

[167] SUÁREZ S., Alberto. La Estafa Informatica. En: Derecho Penal y Criminología. 2006. vol. 27, p. 195

> Dice el artículo 248 del Código Penal español: "1. Cometen estafa los que con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. / 2 También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros. / 3. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo".

Sobre la estafa a través de medios informáticos, ha crecido en mayor proporción, especialmente, debido a que en los últimos veinte años, el comercio electrónico ha pasado de la novedad o conveniencia, a la necesidad. En pocas palabras, en el mundo de hoy, una institución o empresa financiera no puede competir sin la capacidad de realizar transacciones electrónicamente y, aún más, sin la capacidad de transmitir esa comodidad a sus clientes. Las transacciones cara a cara han dado paso a un clic del mouse y a los créditos o débitos instantáneos en la cuenta del cliente que se pueden ver en tiempo real[168].

Pero la conveniencia necesaria también da lugar a nuevos riesgos. Aunque el riesgo de fraude en las instalaciones siempre existirá, desde la perspectiva del desfalcador, la posibilidad de lograr el mismo objetivo sin tener que ser visto está

[168] NADARAJAN, Sivakumar. A Comparative Study of Financial Transaction Cards-Credit & Debit Cards. En: International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2017. vol. 2, no. 6, p. 2456-3307

demostrando llevar consigo un encanto difícil de resistir. Además, la posibilidad de estafar cantidades mucho mayores simplemente ingresando instrucciones desde una computadora también conlleva un incentivo obvio. Aunque uno no es completamente invisible detrás de una pantalla de computadora, el concepto ciertamente está demostrando que da poder y brinda a muchas personas inocuas la confianza para actuar de una manera que probablemente nunca emprenderían si se les exigiera presentarse personalmente ante su víctima[169]

A la luz del auge de las transacciones electrónicas, el fraude relacionado con la informática es una preocupación creciente incluso para las empresas y bancos más pequeños. Los delitos informáticos presentan riesgos reales, y hay mucho en juego para cualquier negocio cuando, en última instancia, un delincuente puede acceder a toda su cartera con solo tocar botones. Las amenazas de apropiación ilícita son mucho mayores que el "hurto" en las instalaciones de una entidad financiera. Con un conjunto de instrucciones de transferencia bancaria robada, una cuenta bancaria extranjera e instrucciones de transferencia de teléfono, correo electrónico o fax, un delincuente puede huir con millones, en prácticamente, un instante, todo desde la comodidad de su hogar. Con el equipo adecuado, el delincuente puede estar algo seguro de que tendrá el tiempo suficiente para escapar antes de que se descubra el ilícito[170].

[169] ANJANEYULU, M y KISHORE, Asst Prof A Uday. Financial Fraud Detection with Anomaly Feature Detection on credit card. En: International Journal of Scientific Research & Engineering. 2019. vol. 5, no. 3, p. 2395-566X

[170] NADARAJAN, Sivakumar.Op. Cit.

Sobre el delito de hurto o estafa por medios informáticos, a medida que las computadoras y dispositivos relacionados, como los teléfonos inteligentes, se han vuelto más comunes, cada vez más, también han sido utilizados por delincuentes. El fraude informático puede incluir la perpetuación de tipos comunes de estafas utilizando herramientas electrónicas, como hacerse pasar por alguien para apropiarse de dinero o datos, o mediante el uso de herramientas electrónicas para promover negocios que son demasiado buenos para ser verdad. Otros tipos de delitos informáticos, a veces llamados delitos cibernéticos, incluyen ataques diseñados para apropiarse ilícitamente y de manera automática, datos de las computadoras, retener Información para el rescate o para evitar que alguien use una computadora.

Así como las herramientas de comunicación más antiguas, como los teléfonos y el correo postal, se pueden utilizar para estafar y defraudar a las personas, también se pueden utilizar herramientas modernas como el correo electrónico, los mensajes de texto y los chats en línea. Los mensajes de correo electrónico que se hacen pasar por remitentes legítimos, como bancos o empleadores, para que puedan apropiarse ilícitamente credenciales como contraseñas y números de cuenta, a menudo se denominan ataques de phishing. Se pueden orientar manualmente hacia destinatarios específicos o se pueden

enviar de forma masiva, con el remitente esperando engañar a los destinatarios incautos para que compartan sus datos personales[171].

El fraude y los delitos financieros son una forma de hurto que ocurre cuando una persona o entidad toma dinero o propiedad, o los usa de manera ilícita, con la intención de obtener un beneficio de ello. Estos delitos generalmente involucran alguna forma de engaño, subterfugio o abuso de una posición de confianza, que los distingue de la apropiación ilícita común. En el ámbito financiero, el fraude y los delitos de esta naturaleza pueden tomar muchas formas comunes de delitos financieros, como falsificación, fraude con tarjetas de crédito, malversación de fondos y lavado de dinero.

El fraude con tarjetas de crédito y débito es una forma de suplantación de identidad que implica una toma no autorizada de la información de la tarjeta de crédito de otra persona con el propósito de cargar compras a la cuenta o eliminar fondos de ella. Este hurto puede ocurrir físicamente cuando se toma la tarjeta de crédito y débito real, o la apropiación ilícita puede ocurrir cuando solo se sustraen los números de un sitio web desprotegido o un lector de tarjetas en una estación de servicio.

Para contener el fraude con tarjetas de crédito, las leyes de los países deben definir con claridad las tipologías y tipificaciones a la luz de las últimas tendencias

[171] ANJANEYULU, M y KISHORE, Asst Prof A Uday. Op. Cit.

del avance tecnológico, a fin de establecer las posibles sanciones que podría enfrentar el delincuente si es declarado culpable del delito.

Al respecto, es conveniente definir los elementos de fraude especialmente con un dinero plástico o tarjetas de débito y crédito. El fraude con tarjetas débito o crédito según ANJANEYULU y KISHORE[172], se puede cometer de varias maneras, como cuando una persona:

- Obtiene, toma, firma, usa, vende, compra o falsifica de manera fraudulenta la información de la tarjeta de crédito o débito o de la tarjeta de otra persona;
- Utiliza su propia tarjeta con el conocimiento de que es revocada o caducada o que la cuenta no tiene suficiente dinero para pagar los artículos cargados; o
- Vende bienes o servicios a otra persona con conocimiento de que la tarjeta de crédito o débito utilizada se obtuvo ilegalmente o se está utilizando sin autorización.

Los tipos de fraude con tarjeta de crédito, a veces denominado fraude crediticio, es un término amplio para el uso de una tarjeta de crédito (o cualquier tipo de crédito comparable) para comprar bienes o servicios con la intención de evadir el pago. Si bien es fácil entender la apropiación física de una tarjeta de crédito o débito de una billetera o cartera, hoy en día es mucho más común que solo se apoderen de información y no la tarjeta en sí. Existen varias formas de fraude con

[172] ANJANEYULU, M y KISHORE, Asst Prof A Uday. Op. Cit.

tarjetas de crédito con métodos nuevos e ingeniosos que se diseñan casi a diario. Los tipos más comunes de fraude crediticio incluyen:

- Abrir nuevas cuentas con identificación suplantada
- Asumir una cuenta existente
- Hacer compras sin que la tarjeta esté presente
- Usando una tarjeta falsificada
- Usando una tarjeta perdida u objeto de hurto[173]

Otra realidad en el ámbito de la estafa o fraude mediante medios informáticos, es la suplantación de identidad, por considerarse una de las formas más dañinas de fraude con tarjetas de crédito, dado que una vez que se toma la información de identificación personal, puede usarse para numerosas actividades fraudulentas. Varios fraudes con tarjetas de crédito dependen de la suplantación de identidad. Cualquier persona que quiere cometer un ilícito, se apropia de la información de identificación de otra persona, puede abrir nuevas cuentas o puede contactar a las compañías de tarjetas de crédito y cambiar las direcciones para hacerse cargo de una cuenta existente[174].

Otro delito que puede dar lugar a la transferencia no consentida de activos, lo constituye la violación de datos. El delincuente puede obtener el número de una

[173] NADARAJAN, Sivakumar.Op. Cit.

[174] ANJANEYULU, M y KISHORE, Asst Prof A Uday Op. Cit

tarjeta. Esto a veces sucede cuando una empresa tiene su información de cliente pirateada en una violación de datos. Las empresas que almacenan la información de la tarjeta de crédito de un cliente a veces tienen esa información apropiada ilícitamente. El delincuente puede usar el número de tarjeta de crédito para hacer compras telefónicas o en línea sin que la tarjeta de crédito esté presente[175].

También existe otra modalidad de delito consistente en una impresión de tarjetas de crédito apropiadas ilícitamente. El ilícito consiste en que cuando se usa tarjeta de crédito, se hace una impresión de la tarjeta en papel carbón. Luego, cuando se desechaba el papel carbón, se podían apropiar ilícitamente de los números de las tarjetas de crédito. Eso no sucede muy a menudo en estos días, pero una versión moderna de eso son los skimmers electrónicos de tarjetas de crédito que pueden leer la información de la tarjeta de crédito de la banda magnética de la tarjeta de crédito. Hay un par de formas de skimmers de tarjetas electrónicas:

- Un tipo es un lector portátil que puede leer tarjetas llevadas en bolsillos y carteras de personas mientras caminan por la calle.
- Otro tipo es un lector que está colocado en una ubicación estacionaria, como un cajero automático o una bomba de estación de servicio. La impresión de la tarjeta de crédito o débito se puede usar para hacer una tarjeta de crédito falsa o falsa que funcionará igual que la real[176].

[175] NADARAJAN, Sivakumar. Op. Cit.

[176] ANJANEYULU, M y KISHORE, Asst Prof A Uday Op. Cit

Para una mayor comprensión el hurto por medios informáticos y semejantes, según el Art. 269I, se señala[177]:

Bien jurídico tutelado la seguridad de los datos y la información y el patrimonio económico.

Es un delito de carácter intermedio porque tiene la doble condición de supraindividual e individual.

Son elementos del mismo la relación posesoria, legitimidad de la relación posesoria, contenido económico de la relación posesoria.

Tipo objetivo este tipo penal es incompleto porque para su configuración remite al artículo 239 del C.P., es decir, al tipo básico del delito de hurto.

Conducta acoge varios factores, 1. Hurto mediante la superación de medidas de seguridad informáticas, la superación de medidas de seguridad informáticas, la manipulación del sistema informático, el apoderamiento de cosa mueble ajena, 2. Hurto mediante la suplantación del usuario.

Sujeto activo es común o de dominio ya que no exige ninguna cualificación.

La autoría mediata se da mediante todas las modalidades de la misma. Permite coautoría.

Sujeto pasivo es un bien jurídico intermedio y los sujetos son dos, la sociedad y el dueño, poseedor o tenedor de la cosa mueble.

Objeto material es real, constituido por la cosa mueble, que en el ámbito penal se denomina la “transportabilidad” para diferenciarlo del inmueble. (incluye el dinero circulante pero no el escritural, contable o documental).

[177] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit.p. 339 y ss

Elementos normativos “ajeno” es lo que pertenece a otro, también son los conceptos de usuario, medidas de seguridad informática, sistema informático, red de sistema electrónico y telemática y sistemas de autenticación y autorización.

Permite tentativa cuando el sujeto activo ejecuta acción idónea para apoderarse de cosa mueble ajena y no logra adueñarse de la misma. Es un delito de resultado, la conducta se consuma cuando el sujeto activo saca la cosa codiciada de la esfera de poder del sujeto pasivo y la lleva a la suya.

Concurso efectivo con otras conductas como las de la información y los datos, el patrimonio económico, la libertad individual y la fe pública. “violación de datos personales”, “suplantación de sitios web para capturar datos personales”, “falsedad en documento”.

Concurso aparente con el delito de “acceso abusivo a un sistema informático”, “secuestro extorsivo”.

Tipo subjetivo es solo de carácter doloso, porque no admite la modalidad culposa.

Por otra parte, los aspectos asociados a la parte objetiva y subjetiva del injusto en el caso de la transferencia no consentida de activos, será abordada en el próximo capítulo.

E. Ley No. 1928 de 24 julio de 2018

Colombia, con todo su avance tecnológico, la expansión del uso del Internet a nivel territorial, la consolidación del Ministerio de las TIC, se encontraban en mora de ratificar el convenio sobre la ciberdelito en Budapest, muy a pesar de haber sido invitada desde el 11 de septiembre de 2003. Es mediante la ley número 1928

24 de julio de 2018, que se promulga la ley por medio de la cual se aprueba el “convenio sobre la ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. En la exposición de motivos de la Ley 1928 (2018), se afirma que:

> El crecimiento de las amenazas en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado. Esto lo que pone de manifiesto es la necesidad de desarrollar de forma estricta políticas de seguridad necesarias para establecer controles que permitan proteger tanto a la ciudadanía sociedad, como al Estado y sus infraestructuras críticas, ante estas nuevas amenazas. Tales políticas de seguridad han de ser respaldadas por un adecuado marco normativo sustancial y procesal de naturaleza penal, para que su implementación sea efectiva[178].

Los profundos cambios en el mundo global han provocado la digitalización, convergencia y globalización continua en las redes informáticas y sociales. Colombia adopta este convenio con el fin de intensificar la cooperación internacional frente al delito informático y hacer parte con carácter prioritario de una política penal común encaminada a proteger a la sociedad frente a ciberdelincuencia.

[178] Exposición motivos del proyecto de ley, por medio cual aprueba el «convenio sobre la ciberdelincuencia», adoptado 23 noviembre de 2001, en Budapest, p.1

Al tenor del Convenio de Budapest, cabe resaltar que su articulado contiene en primera instancia la legislación sustantiva tendiente a construir una política criminal común, encaminada a sancionar la criminalidad en el ciberespacio, estipulado en los artículos 2 a 12, lo cual implica a los Estados “adecuar su legislación interna a las exigencias estipuladas en dichos instrumentos, relativas a los temas de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual, y responsabilidad de las personas jurídicas” según la exposición de motivos de la Ley 1928 (2018).

Por otra parte, el Convenio de Budapest contempla la legislación procesal, en los artículos 16 a 21 de dicho convenio, que obliga a las autoridades públicas de los diferentes Estados adoptantes, adecuar la legislación procesal en los siguientes aspectos:

a) Adoptar medidas para garantizar la conservación inmediata de “datos informáticos almacenados” y la divulgación de los denominados “datos de tráfico”.
b) Otorgar facultades a las autoridades competentes, para que puedan solicitar a los proveedores de servicios y demás particulares la entrega de datos almacenados en su poder.
c) Disponer de medios idóneos para interceptar y compendiar en tiempo real "datos de tráfico" asociados con una comunicación particular.
d) Expedir la regulación pertinente, que habilite a sus autoridades a acceder y decomisar cualquier sistema o soporte de almacenamiento informático. Exposición de motivos de la Ley 1928 (2018)

El tercer aspecto del Convenio de Budapest está asociado a la necesidad de la cooperación internacional, con el principal instrumento para la lucha contra el delito informático y la ciberdelincuencia, en el sentido de facilitar su detección, investigación y sanción tanto en el ámbito nacional como internacional, a través de procedimientos de cooperación de manera rápida y fiable, respetando el derecho interno pero ajustado el marco internacional del convenio.

Finalmente, el acuerdo de adopción frente al Convenio de Budapest establece ciertas reservas al tenor del artículo 14 del tratado, con el objeto de proteger los derechos constitucionales del *habeas data* y la intimidad personal. Según la exposición de motivos de la ley Ley 1928 (2018), se señala que:

> En dicho postulado normativo se faculta a los Estados a reservarse el derecho de aplicar las medidas establecidas en el artículo 20 del Convenio relativo a “Obtención en tiempo real de datos relativos al tráfico", pero únicamente para ciertas categorías de delitos especificados en la reserva. También se plantea la posibilidad de reservar la aplicación del artículo 21, concerniente a la “interceptación de datos relativos al contenido" en los casos en que un sistema informático:
>
> - Se haya puesto en funcionamiento para un grupo restringido de usuarios
>
> –No emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado. Estas

> reservas protegerían posibles vulneraciones a derechos establecidos como fundamentales en la Constitución Política de Colombia ampliamente desarrollados por la Corte Constitucional[179]

Con respecto a la constitucionalidad de la Ley No. 1928 de 24 julio de 2018, la Corte Constitucional[180] señala en sus conclusiones de fallo que: El Convenio sobre la Ciberdelincuencia se presenta como un instrumento internacional cuyo objetivo es intensificar la cooperación entre los Estados Parte del mismo, mediante la materialización de una política criminal común en contra de la comisión de delitos cibernéticos. Lo anterior, como una respuesta a los profundos cambios provocados por la digitalización, convergencia y globalización de datos y sistemas informáticos. De esta manera, al establecer las condiciones para prevenir la comisión de ilícitos en las redes informáticas, compromete a los países signatarios a adoptar su legislación interna para combatir posibles amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de datos y de los sistemas informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

La totalidad de las disposiciones contenidas en el Convenio conservan como base la cooperación entre las Partes, lo cual es un desarrollo del tratamiento igualitario y los efectos recíprocos del Convenio. Destaca la Corte que lo contenido

[179] Ibid. p.6

[180] Corte Constitucional, Sentencia C-224/19, Revisión oficiosa de la Ley 1928 de 2018 “Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest”.

en este instrumento efectiviza los fines esenciales de la Constitución, atiende la soberanía e independencia del Estado colombiano en materia penal, y observa los mandatos constitucionales que se concretan con la adquisición de compromisos internacionales regidos por principios de conveniencia, soberanía nacional, reciprocidad y equidad.

Asimismo, la Corte encuentra ajustado a la Constitución la disposición sobre la reserva anunciada por Colombia, mediante la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Internacionales, como Estado Parte del Convenio sobre la Ciberdelincuencia, en el entendido que, por su intermedio, se propende por la defensa de los derechos fundamentales a la intimidad y al *habeas data*. La reserva a la que se acogerá el Estado colombiano, prevista en el numeral 3 del artículo 14 del Convenio, deberá ajustarse a los términos de la Constitución Política de 1991. En mérito de lo expuesto, la Corte Constitucional de Colombia, resolvió declarar exequible el *"Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, Hungría* y en ese mismo término, declarar exequible la Ley 1928 de 2018, "por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, Hungría".

La importancia de la transferencia no consentida de activos tipificada en el Código Penal colombiano, al tenor de la constitucionalidad Ley No. 1928 de 24 julio de 2018 se aborda en el siguiente capítulo.

CAPITULO III. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS EN COLOMBIA Y EL DERECHO COMPARADO

A. Contextualización jurídica

Dentro de la gama de delitos informáticos que se cometen en el país, llama la atención la llamada estafa o movilidad de activos sin consentimiento, especialmente cuando se refiere a la afectación de las transacciones financieras a través de las diferentes entidades de intermediación. Si bien en Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", aún existen vacíos jurídicos desde el punto de vista del Código Penal, que se hace necesario analizar y profundizar para lograr incorporar su modernización acorde a las nuevas modalidades del ciberdelito, dado que, retomando lo anteriormente comentado, la expansión del Internet ha generado una serie de actividades delictivas que afectan a las empresas, las personas y la sociedad en general, tal como lo señala BARRIOS A[181]., al afirmar que:

> A la postre, la expansión de Internet ha provocado, a la vez, una aparición de un elenco de actividades nocivas para los ciudadanos, algunas de las cuales producen la lesión de bienes

[181] BARRIOS A., M.Op. Cit. p.19

> jurídicos relevantes protegidos por el Derecho Penal[182]. Por lo general, un número importante de estas actividades constituye una peculiar adaptación al espacio virtual de conductas lesivas más o menos clásicas desde la perspectiva penal, para cuya ejecución se aprovecha la viralidad y globalidad de este canal de comunicación (como ocurre, por ejemplo, con las estafas).

Dado que uno de los objetivos de esta investigación monográfica está orientado al análisis de la transferencia no consentida de activos, al tenor del Código Penal, el cual señala en su artículo 269J lo relacionada con la defraudación informática económica, que consiste en la Transferencia no consentida de activos, de la siguiente forma:

> El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes"[183].

---

[182] A los efectos del Derecho Penal, existen determinadas técnicas y modos de proceder cibernéticos constitutivos de ilícito penal (por ejemplo, acceso inconsentido a un sistema informático, interceptación ilícita de comunicaciones, interferencias en el sistema, prácticas de *phising*, ataques de denegación de servicio —D*o*S—, abuso de dispositivos, fraude informático, etc.) y también ciertos contenidos cuya vulneración se ve facilitada por el medio Internet (v. gr. delitos de pornografía infantil, contra la propiedad intelectual e industrial o revelación de datos personales). Citado por BARRIOS A., M.Op. Cit.

[183] Al respecto CB, Ch. I, art. Article 8–Computer-related fraud, citado por (R. Posada M., 2012) "(...) cuando se produzcan intencionalmente y sin derecho, una pérdida de propiedad a otra persona por: una entrada, alteración, borrado o supresión de datos informáticos; b cualquier interferencia con el funcionamiento de un sistema informático, con intención fraudulenta o

Sobre el mencionado artículo, los expertos han señalado desde el punto de vista doctrinal su análisis detallado con respecto al alcance y aplicación al tenor de la jurisdicción del Estado colombiano.

> Se trata de una modalidad típica diferente a la estafa tradicional (CP/art. 356)[184], porque, aunque comparte algunos de sus elementos dogmáticos (objetivos y subjetivos), se caracteriza por sancionar operaciones automáticas realizadas por sistemas informáticos como resultado directo de manipulaciones defraudadoras impulsadas, desarrolladas o ejecutadas por el sujeto activo[185]

En este contexto, es importante analizar desde la perspectiva del código penal, como Colombia ha querido hacer frente a las grandes amenazas del ciberdelito y que por lo tanto hay necesidad de analizar el tema desde el derecho y las ciencias jurídicas, a fin de contribuir a la comprensión de este fenómeno global

---

deshonesta y sin derecho, un beneficio económico para sí mismo o para otra persona" (T/L). El supuesto de hecho doméstico es una copia, aunque en otro contexto de protección, de la norma prevista en el CP de España/art. 248.2. A diferencia de este, allí se le considera de modo exclusivo un delito patrimonial.

[184] Según (R. Posada M., 2012), su naturaleza es muy disputada. Por una parte, se encuentran aquellos doctrinantes que afirman que la transferencia es una modalidad asimilada al tipo básico de estafa o un tipo especial de estafa (Orts Berenguer et al, 2004, p. 571), quienes hablan de estafas cometidas dentro y fuera del sistema; Serrano Gómez et al (2009, p. 435, hablan de estafa peculiar), por la otra, quienes sostienen que se trata de un tipo informático autónomo defraudatorio (Borja Jiménez 2003, p. 307; Faraldo Cabana 2009, p. 85; Polaino Navarrete et al, 2011, p. 98; Quintero Olivares et al 2011, p. 668, porque pretende criminalizar conductas lesivas para el patrimonio ajeno extramuros de la dinámica comisiva presidida por el engaño; Suárez Sánchez 2011, p. 245, entre otros autores).

[185] POSADA M., Ricardo. Op. Cit. p. 8

que afecta a la sociedad actual, especialmente la transferencia no consentida de activos, tipificado en el código penal art. 269J, como “El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes” pero que en otros países, excepto España y Ecuador, no se conoce así, sino bajo otras modalidades de estafa informática.

El Código Penal al ser modificado por la Ley 1273/2009 incluyó un capítulo sobre delitos informáticos, en respuesta a la Convención de Budapest sobre Cibercrimen, que fue aprobada mediante la Ley 1928/2018 y adoptada en noviembre de 2018. La convención aborda asuntos relacionados con delitos cometidos a través de Internet y otras redes informáticas, que incluyen:

- Violaciones de derechos de autor;
- Pornografía infantil; y
- Violaciones a la seguridad de la red.

Una de las tantas actividades cibernéticas que están criminalizadas en Colombia, es la transferencia no autorizada de activos. Ahora bien, la ley Ley 1273

de 2009, conocida como ley de delitos informáticos, ha sido concebida según. SALAZAR[186] (2011) como:

> Una norma disuasoria contra la criminalidad electrónica, redundando en mayor confianza del público en el uso de los medios electrónicos. Solo con la cabal aplicación de las penas consagradas en la Ley se sentarán precedentes que no permitan que Colombia se convierta en un paraíso de la delincuencia informática, como lo ha sido respecto de otras formas de criminalidad.

Por su parte, MANJARRÉS Y JIMENEZ T[187]., sobre la importancia de la norma en términos de combatir el ciberdelito en sus diferentes manifestaciones dado el avance de las tecnologías y el Internet, dentro del marco del convenio sobre cibercriminalidad suscrito en Budapest en el año de 2001, sostienen que:

> Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los “delitos informáticos”, con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el

[186] SALAZAR, Juan Fernando. Op. Cit. p. 101

[187] MANJARRÉS, B., I. y JIMENEZ T., F. p.78

> Convenio ‘Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

B. Sujetos del delito informático

Para comprender el alcance del delito sobre transferencia no consentida de activos, es menester definir los sujetos que actúan en la comisión de un delito, en este caso los delitos relacionados con el cibercrimen, identificando en primera instancia quien es el sujeto activo o persona que actúa haciendo uso de los sistemas informáticos, que posee habilidades especiales y competencias para cometer un delito informático frente al sujeto pasivo que viene siendo la persona afectada sobre la cual recae la acción ilícita de sujeto activo, que en otras palabras viene siendo la víctima en su modalidad individual, institucional, corporativo o entidad gubernamental.

Al respecto, MANJARRÉS y JIMENEZ T[188]., define el sujeto activo como:

> Las personas que cometen los “Delitos Informáticos” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los

[188] MANJARRÉS, B., I. y JIMENEZ T., F. Op. Cit. p. 75

sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con respecto a la caracterización del sujeto pasivo o víctima de estafa, dado que posee la titularidad del bien jurídico protegido, el mismo autor MANJARRÉS y JIMENEZ T.[189], lo define como:

> El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos” las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

Comprender el sujeto pasivo es muy importante en cuanto a través de él se puede conocer diferentes ilícitos cometidos por el delincuente, muchos de los cuales son identificados casuísticamente, debido al desconocimiento del modus operandi del delincuente, tras el uso de diferentes formas y dispositivos

[189] Ibid. p. 75

tecnológicos, dado el avance y desarrollo de las tecnologías en diversos campos del quehacer de la sociedad.

Con estas premisas definitorias, se puede abordar el contexto del delito de transferencia no consentida de activos, tipificado en el Código Penal Colombiano

C. Aspectos dogmáticos de la transferencia no consentida de activos

La transferencia no consentida de activos, es un tipo de delito de defraudación económica a través de medios informáticos, donde el delincuente tras el ilícito se lucra del bien ajeno manipulando un dispositivo informático, en perjuicio de un tercero, constituyendo una modalidad diferente a la estafa tradicional, por cuanto si bien comparte algunos elementos dogmáticos objetivos y subjetivos, la comisión del delito se realiza de manera automática por medio informático directo de manipulaciones con fines probatorios ejecutada por un sujeto activo[190].

En la transferencia no consentida de activos, el sujeto activo posee especiales conocimientos técnicos en materia informática “Incluso, el sujeto activo puede ser el titular legítimo del sistema cuando lleve a cabo una manipulación informática a su favor y en perjuicio de otro (Rovira del Canto, 2002, p. 565). De todas maneras, no se puede confundir el sujeto activo del tipo con el beneficiario de la acción criminal, pues la práctica enseña que, ocasionalmente, los

[190] POSADA M., Ricardo.Op. Cit.

beneficiaros no son quienes realizan la conducta punible y, en muchos casos, ni siquiera están al tanto de la defraudación"[191].

En la transferencia no consentida de activos[192] el bien jurídico tutelado es la seguridad de los datos y la información y el patrimonio económico, porque la ejecución del ilícito no solo produce daño al bien jurídico del patrimonio individual (activos), sino que también a la confidencialidad, integridad y disponibilidad de los datos[193], en razón al bien protegido.

Para la consumación de la conducta punible y su reproche, no basta con que se ponga en peligro el bien jurídico tutelado, es decir, el patrimonio económico, pues se requiere igualmente que se cause peligro para el bien jurídico supraindividual que para este caso puntual lo constituye la seguridad de la información en los medios informáticos que han sido objeto de manipulación informática o artificio semejante. Por ello, este delito tiene la doble condición de supraindividual o colectivo e individual, siendo de los denominados delitos intermedios, toda vez que el comportamiento típico lesiona de inmediato el bien jurídico asociado al adecuado funcionamiento de los sistemas de información y los

[191] POSADA M., Ricardo.Op. Cit. p. 9

[192] SUÁREZ S., A., citando a MATA Y MARTÍN. *Delincuencia informática*, 2001. p. 53, concluye que, hay transferencia de activos a pesar de que el autor no llegue materialmente a recibir nada o no reciba anotación en su propio patrimonio, como cuando lo que hace es realizar una anotación contable con la que salda una deuda, de forma que en este caso también recibe un beneficio patrimonial y causa el perjuicio correspondiente. Cit. Pie de página. Manual de Delito Informático en Colombia. 2016. p. 385

[193] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 372

datos –bien jurídico intermedio supraindividual- y de forma mediata afecta o pone en riesgo el patrimonio económico previsto como bien jurídico intermedio individual[194].

En cuanto al objeto jurídico, corresponde al titular de la información en condición de sujeto pasivo, caracterizado por la posibilidad de acceder, disponer, transferir y conocer, de manera libre, acerca de sus datos de información de carácter económico representados en activos patrimoniales[195]. El bien jurídico en este caso es intermedio y los sujetos son dos, la sociedad en cuanto al interés supraindividual y el titular del activo objeto de la transferencia no consentida, con relación al bien jurídico individual.

El objeto material sobre el cual recae la acción, es tipo inmaterial determinable, la transferencia de los datos representados en activo patrimonial de cualquier naturaleza, de valor monetario perteneciente a una persona o entidad corporativa[196].

Dada la fenomenología del delito, como conducta presenta dos modalidades de comportamiento alternativo a saber; por una parte, la

[194] Ibid. p. 373 y ss

[195] POSADA M., Ricardo.Op. Cit. p. 11

[196] Ibid.

transferencia no consentida de activos y en segunda medida la fabricación y el tráfico de programa de computador malicioso[197].

En lo referente a la transferencia no consentida de activos, el comportamiento típico esta antecedido del vocablo “valerse” y se complementa señalando unas modalidades abstractas y genéricas como son; la manipulación informática y el artificio semejante. La segunda forma de cometer el delito, es una clausula general de extensión del ámbito típico establecido por la primera. Por consignar dos formas punibles opcionales la transferencia no consentida de activos acoge los aludidos tipos mixtos alternativos, porque el concurso de sus modalidades solo permite tipificar delito único, dado que si el autor realiza una manipulación informática y un artificio semejante a la vez, no se puede contemplar la comisión de dos delitos diferentes de transferencia no consentida de activos en concurso, si no solo la de uno[198].

SUÁREZ S., A.[199], entiende la manipulación informática como aquella conducta que incide en un sistema informático provocando su incorrecto funcionamiento, o la que implica un incorrecto uso del mismo, esta puede incidir en cualquiera de las fases del sistema siempre que sea idónea para lograr la transferencia no consentida del activo patrimonial, ya sea en la introducción de

[197] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 373

[198] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 374 y ss

[199] Ibid. p. 376

datos para que opere el mismo o cuando finalizado el proceso se emitan sus resultados al exterior a través de algún medio impreso, visible en la pantalla u otra forma de transmisión de datos a diferentes ordenadores conectados en red, causando la transferencia y la afectación al bien jurídico en cabeza del sujeto pasivo.

La manipulación del sistema informático a menudo suele realizarse desde diferentes lugares y con frecuencia acudiendo a terminales móviles que facilitan la suplantación de datos y evitan la identificación de la red previendo no ser asociada a determinado operador.

Existen múltiples modalidades de engaño que permiten acceder a los datos privados de otros usuarios los cuales posteriormente pueden ser utilizados con fines económicos y para el caso de la transferencia no consentida de activos como medio para ejecutar el delito, una de las más conocidas en el delito a través de medio electrónico es el "*phishing*"[200] del cual BENÍTEZ ORTÚZAR[201] genera algunas categorizaciones en los siguientes términos:

[200] El *Phishing***:** es un tipo de estafa informática que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, esto es, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas, a fin de adquirir una contraseña o información detallada sobre tarjetas de crédito o números de cuentas bancarias. Cit. GRISALES PÉREZ. G., En: Revista derecho penal n°:48, jul.-sep./2014

[201] BENÍTEZ ORTÚZAR, I. F., "Informática y delito. Aspectos penales relacionados con las nuevas tecnologías". En: MORILLAS CUEVA, L. y CRUZ BLANCA, M. J., Reforma del Código Penal. Respuestas para una sociedad del siglo XXI, ed. Dykinson, Madrid, 2009, pp. 111 y ss. [En línea]: http://www.eumed.net/libros-gratis/2014/1397/tecnologia-delito.html#_ftn24

- Phishing sobre Web falsas de recarga de móviles: con llamativas ofertas de descargas más económicas con el objetivo de hacerse a la información del usuario.

- Phishing a través de la propia Web: con la suplantación de la página Web de una entidad financiera ("Web spoofing") obtienen los datos bancarios con los que después operan.

- Phishing laboral o "Scam": oferta falsa de trabajo, con el objetivo de obtener la cuenta bancaria del destinatario y utilizarla luego para blanquear dinero a nombre de ésta.

- Phishing-car: oferta de vehículos de lujo a bajo coste solicitando una cantidad económica para la entrada.

- Phishing de las loterías falsas: mediante un correo comunicando al destinatario que ha ganado un premio de lotería. Si éste contesta, se le solicitan los datos bancarios para el falso ingreso del dinero.

En la transferencia no consentida de activos es frecuente el uso de "*pharming*" el cual resulta más efectivo y difícil de descubrir ya que se pone en

práctica a través de la utilización de virus[202], gusanos[203], troyanos[204], bombas lógicas[205] y programas espías que logran hacer una intrusión a los computadores de las víctimas para sustraer de ellos la información privilegiada que se requiere a fin de vulnerar el patrimonio económico o la información personal privilegiada[206].

En cuanto al "artificio semejante" existen diferentes posiciones interpretativas, por lo tanto resulta complejo establecer una definición integral, pues en sentido amplio la norma no considera en que termino debe ser semejante el artificio a la "manipulación informática". Algunos autores como QUERALT

[202] El virus informático: es un malware que tiene por objeto alterar el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un computador.

[203] Gusano: este tipo de software no busca principalmente la destrucción de datos, sino su autorreplicación y transmisión para interferir la función informática de otros ordenadores. Su campo de actuación es la red.

[204] Troyano: Es un programa informático malicioso para robar contraseñas. Es un software malicioso que, oculto en un programa benigno o útil, se introduce en el sistema informático (incluso en teléfonos móviles o PDA´s). Una vez dentro del sistema, puede generar un gran número de disturbios o daños en este (borrado o daño en los datos o programas, utilizar el sistema para realizar ataques de denegación de servicios, robar contraseñas y datos, abrir "puertas traseras" para permitir a los atacantes controlar el sistema y convertir el ordenador en un zombi al servicio de estos). Actualmente son las principales amenazas sobre los ordenadores.

[205] Bomba lógica: son rutinas introducidas en un programa para que al realizar una determinada acción —por ejemplo, copia de este—, se produzcan alteraciones o daños en el programa. Las bombas de tiempo como las lógicas, son rutinas introducidas en programas o archivos, pero para que se produzca una alteración del programa o daño a este en un momento determinado, al llegar a una fecha concreta o pasar un plazo de tiempo establecido al efecto.

[206] GRISALES PÉREZ. Giovanni. Hurto por medios informáticos y transferencia no consentida de activos en Colombia. 2014. En: Revista derecho penal n°:48, jul.-sep./2014, págs. 121-189

JIMÉNEZ[207] han tenido una aproximación con el tema concibiéndolo de la siguiente forma:

> El artificio semejante es la alteración de los datos contenidos en el ordenador y afirma que la manipulación informática en sentido estricto seria la modificación de los programas que gestionan, en todo o en parte, el proceso de transferencia de activos de una base de datos a otra, por lo que considera que tienen cabida dentro de tal concepto las manipulaciones del hardware si se consigue el fin propuesto. En todo caso, estima que para hacer la introducción de tales datos, conducta que quedaría cobijada por el denominado "artificio semejante", ha de manipularse por lo general de manera previa el sistema informático, o haberse producido al menos una interceptación de las líneas de comunicación, razón por la cual se debe tener en cuenta que "el artificio análogo (o artificio semejante, según la denominación de la ley) es una variante de la alteración informática (manipulación informática).

Por su parte, FARALDO CABANA[208] al analizar el delito de transferencia no consentida de activos, es contundente en afirmar que "la única forma de reducir la excesiva extensión de la conducta típica consiste en entender que el artificio que

[207] QUERALT JIMÉNEZ, J., PE, 2008, p. 491. En: SUÁREZ S., A. Manual de Delito Informático en Colombia. Análisis dogmático de Ley 1273 de 2009. Bogotá: Universidad Externado de Colombia, 2016, p. 380

por exigencia legal debe ser semejante a la manipulación informática, ha de suponer el empleo de tecnología avanzada, necesariamente informática". En ese entendido, "el artificio ha de ser semejante a la manipulación informática, esto es, la expresión utilizada por el legislador debe entenderse en el sentido de un «artificio informático semejante», y no en el sentido de un «artificio no informático semejante»".

La segunda modalidad asociada con la fabricación y el tráfico de programa de computador malicioso es definida por SUÁREZ S., A.[209], argumentando que, son típicos de esta modalidad los comportamientos de fabricar, introducir al territorio nacional, poseer o entregar el objeto material constituido por programa de computador destinado a la manipulación informática o la realización de artificio o engaño para inducir a error a otro y obtener provecho económico con perjuicio ajeno. El programa de computador es el conjunto de instrucciones que la CPU de un ordenador puede entender y ejecutar. El delito se consuma cuando el programa malicioso tenga como finalidad ser destinado a la manipulación informática propia

---

[208] FARALDO CABANA. Patricia. Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico, p. 104 – 105. En: Revista de Derecho Penal y Criminología, 3.a Época, n.º 3 (2010)

Según (P. Faraldo C.,), destacando la importancia de que se exija una semejanza entre los artificios y las manipulaciones informáticas, Mata y Martín, R. M., Delincuencia informática, cit., pp. 48-49. Vid. también Anarte Borrallo, E., «Incidencia», cit., p. 233. Afirma que con la expresión «artificio semejante» se hace referencia a la manipulación de «soportes electrónicos o telemáticos», Suárez González en Rodríguez Mourullo, G. (Dir.), Comentarios, cit., p. 711; añaden a éstos los ficheros informáticos, electrónicos o telemáticos y los soportes informáticos Vives Antón/González Cussac en Vives Antón, T. S. (Coord.), Comentarios, II, cit., p. 1238.

[209] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 393

de la transferencia no consentida de activos o la realización de delito de estafa, sin que sea necesario su uso por quien lo tenga en su poder.

El tipo penal objetivo de la transferencia no consentida de activos es autónomo y se encuentra determinado por el articulo 269J del Código Penal como: “El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave”.

En cuanto al tipo subjetivo, la transferencia no consentida de activos es solo de carácter doloso, ya que no admite la modalidad culposa, por lo cual, para que se materialice el desvalor de resultado deben concurrir en el sujeto activo los elementos cognoscitivo y volitivo, es decir, el individuo debe tener pleno conocimiento de la ilicitud de su comportamiento al no hallarse autorizado por el titular del bien jurídico –activo patrimonial- para transferirlo y en ese mismo sentido, el infractor debe tener la voluntad de decidir y ejecutar la conducta.

Otro aspecto esencial en la transferencia no consentida de activos es el ánimo de lucro, calificado como un elemento fundamental de carácter subjetivo para la adecuación típica del ilícito, pues en todo caso, este debe acoger un factor patrimonial.

Es importante destacar que en el evento en que el sujeto actué con error de que su comportamiento le es permitido, bajo la creencia que está facultado para llevar a cabo la transferencia del activo patrimonial, en estos casos puede concurrir el error de tipo del que habla el articulo 32 numeral 10 de la Ley 599 de 2000 para el caso colombiano[210].

En cuanto al sujeto pasivo, hace referencia al titular del bien jurídico considerado como patrimonio económico, con datos informatizados de valor contable, lo cual puede ser extensivo a una persona de naturaleza jurídica, que a su vez son víctimas al ser perjudicados en su patrimonio económico por la acción del sujeto activo[211].

El resultado del ilícito, es de naturaleza penal por cuanto afecta al sujeto pasivo en su patrimonio o información que representa dinero escriturado contable, no autorizada y no consentida por su titular en perjuicio de un tercero[212].

Los elementos normativos que rodean el delito analizado son la "manipulación informática", "artificio semejante", "transferencia no consentida", "activo", "perjuicio" y "programa de computador" como se explicó anteriormente.

---

[210] El Código Penal de Colombia considera que: No habrá lugar a responsabilidad penal, cuando se obre con error invencible de que no concurre en su conducta un hecho constitutivo de la descripción típica o de que concurren los presupuestos objetivos de una causal que excluya la responsabilidad".

[211] POSADA M., Ricardo.Op. Cit. p. 10

[212] Ibid. p. 18

El delito de transferencia no consentida de activos permite la tentativa que se da a partir del comienzo de la manipulación informática, es decir, desde la superación, con ánimo de lucro, de los medios de protección de los sistemas informáticos, lo que ya es un acto ejecutivo. Por ser un delito de resultado, se requiere que el sujeto activo cause perjuicio económico a un tercero como consecuencia de la transferencia hecha mediante la manipulación informática[213].

Si el perjuicio no se consuma dado el comportamiento voluntario ejecutado por el autor posterior a la manipulación informática no devendrá responsabilidad penal por dicha tentativa, pues su desistimiento es voluntario. Sin embargo, esto no implica ausencia de responsabilidad en los casos en que el sujeto ha consumado otros delitos que anteceden la manipulación informática como el acceso abusivo a un sistema informático o daño informático, pues en tal caso sería responsable de los mismos[214].

En ese orden de ideas, deben ser inequívocos los actos ejecutivos orientados a manipular el sistema informático pretendiendo transferir los activos, pues solo así, se podría predicar la tentativa de transferencia hasta el momento en el que se "consigue" el traspaso fáctico de los activos patrimoniales, pues de concurrir dichos presupuestos, se estima que la obtención de fondos afecta el bien

[213] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 398

[214] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 398

patrimonio económico del sujeto pasivo. Por el contrario, si se acoge la segunda posición jurídica, la obtención del traspaso de activos seguiría siendo tentativa del delito hasta que no quede perfecta la operación comercial mediante la correspondiente anotación contable informática[215].

En la transferencia no consentida de activos se da la autoría mediata[216] prevista en todas las modalidades de la misma, entendiendo que el artículo 29 del Código Penal es claro en señalar que “es autor quien realice la conducta punible por si mismo o utilizando a otro como instrumento”, es decir, tal y como lo describe SUÁREZ S., A[217], el autor directo o inmediato unipersonal, el mediato y el coautor, de quienes el legislador ha considerado que tienen merecimiento del mismo marco penal por el delito consumado o intentado reconoce estas formas de concurso como autenticas formas de autoria, quedando claro que la autoria es una cuaestion tanto de la parte general como de la especial del Código Penal.

Para el caso de la coautoría[218], esta susbsite en la tranferencia no consentida de activos cuando hay un acuerdo común con división de trabajo

[215] POSADA M., Ricardo.Op. Cit. p. 15

[216] La autoría mediata es considerada una forma de autoría que se identifica por la comisión de un delito a través de otra persona. En ese sentido, el autor mediato es aquel que comete el delito sirviéndose de otro como "Instrumento" humano. La autoría mediata en términos generales extiende la noción de autor que comúnmente acoge la ejecución de propia mano del tipo.

[217] SUÁREZ S., A. Autoría., 3.ª ed. Universidad Externado de Colombia. 2007. p. 248

[218] La coautoria supone una ampliación de la responsabilidad penal descrita en el art. 29, inc. 2 del C.P. Col.,a traves de la cual se puede calificar como autores a quienes puestos de acuerdo para la realización del delito sólo llavan a cabo una parte de la conducta descrita en el tipo, dado que sus aportes son incompletos y sólo con su suma se puede llegar a la produicción del resultado. Como

criminal atendiendo la importancia del aporte orientado a general lesion del bien juridico tutelado –activo patrimonial- en perjuicio de un tercero.

En cuanto al concurso de delitos en la tranferencia no consentida de activos, por tratarse de un delito informático existe “la posibilidad de repetición de la acción delictiva que estimula la permanecia en la comisión del hecho”; de igual forma, podría ocurrir que con una sola acción en la manipulación informática o la modificación en la base de datos se afecte el sistema operativo que procesa, almacene o transfiere datos y por ende se presente la repetición automatizada del comportamiento ilícito, lo cual permite el concurso con el delito continuado y delito masa[219], al concurrir una pluralidad de acciones que transgreden el mismo precepto, para el caso en concreto, mediante la “plurar transferencia de activos lesiva para el mismo sujeto pasivo”.

De igual forma, la transferencia no consentida de activos permite el concurso efectivo con el delito de violación de datos personales y suplantación de sitios web para capturar datos personales, fundamentamente porque el sujeto activo de la conducta a traves de engaño puede lograr el ingreso del sujeto pasivo a un dominio de red diferente al legalmente constituido y aceptado para sus

---

cada uno de los intervinientes lleva a cabo una acción típica en el caso de que el tipo describa una accion típica, o cada uno lleva a cabo una o parte de una de las acciones típicas de las varias que describen el tipo, o todos cumplen cada una de las acciones típicas que integran el tipo, se autoriza que a todos ellos se les impute como propios los aportes de los demas, en razon del denominado principio de imputación reciproca. (SUÁREZ S., A. Autoría. p. 349 – 350. Cit. Gutiérrez Rodríguez. La responsabilidad penal, cit., p. 74)

[219] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 400 y ss

transacciones, haciendole incurrir en error y apoderandose de sus datos personales, que luego son utilizados en la tranferencia de activos en perjuicio de su patrimonio económico.

En lo relacionado con el concurso aparente de delitos la transferencia no consentida de activos puede concurrir con el acceso abusivo a un sistema informático, daño informático y uso de software malicioso, si consideramos que el autor del hecho para asegurar la tranferencia no consentida del activo debe adelantar la manipulación informática o artificio semejante mediante el acceso abusivo al sistema de información, generar el daño, alteración o desaparición de datos y producir y traficar el uso de programas de computación con efectos nocivos, según corresponda en cada caso, sin embargo, es aparente ya que el "principio de consumación" y el "desvalor"[220] de la tranferencia no consentida de activos, recoge los elementos típicos[221] y desplaza los otros delitos.

[220] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 404 y ss

[221] REYES ECHANDÍA expresa que es el fenómeno según en virtud del cual una misma conducta parece subsumirse a la vez en varios tipos penales diversos y excluyentes, de tal manera que el juez no pudiendo aplicarlo coetáneamente sin violar el principio del non (ne) bis in idem debe resolver concretamente a cuál de ellos adecua al comportamiento (parecido al concurso ideal). Para REYES ALVARADO (su hijo), plantear que el concurso aparente es una manifestación de la unidad delictiva en la cual varias normas describen esa misma conducta hace pensar en que no es correcto que reconociendo de antemano la existencia de una sola acción que sólo puede generar una sanción penal, puedan concurrir una pluralidad de disposiciones que comprendan ese comportamiento dentro de su descripción; pues bien, esta afirmación es correcta y pone de relieve que lo que se ha venido denominando concurso aparente de hechos punibles es en la mayoría de los casos es producto de fallas legislativas que suelen derivarse de la equivocada pretensión legislativa de sancionar conductas de acuerdo con la forma de lesión del bien jurídico protegido en lugar de tener en cuenta sólo la efectiva afectación al bien jurídico y el grado en que dicha lesión se haya producido" (El concurso de delitos. Temis: Bogotá, 1990, página 97)

Por tratarse de un delito de resultado, en la transferencia no consentida de activos se puede dar la comisión por omisión cuando la protección del bien jurídico este a cargo de un agente cualificado garante de salvaguardar el mismo, para evitar que se cause daño a un tercero, tal y como lo señala SUÁREZ S.[222]

> Es viable la comisión por omisión, siempre y cuando que quien omite tenga la obligación de actuar, conforme a lo establecido por el inciso 2 del artículo 25 del Código Penal. Esto porque, como antes se dijo, el tipo penal no señala de manera expresa que tal manipulación deba realizarla el mismo autor del delito, dado que el art. 269I se limita a exigir que aquel consiga la transferencia no consentida "valiéndose de alguna manipulación informática o artificio semejante", y bien puede ocurrir que el sujeto agente se sirva de la manipulación que otro realice para producir la transferencia y el perjuicio.
>
> Para que la omisión sea considerada constitutiva del delito de transferencia no consentida de activos, hay que acudir al artículo 25 del Código penal a fin de apreciar la denominada omisión impropia de los delitos de resultado, pues para calificar dicha transferencia como delito de comisión por omisión, se exige que su autor se encuentre en una situación especial con relación al bien jurídico tutelado, que le imponga una posición de garante respecto de los posibles daños patrimoniales, posición que le obliga a realizar una conducta encaminada a evitar dichos resultados.

[222] SUÁREZ S., A. Manual de Delito Informático en Colombia. 2016. Op. Cit. p. 394 y ss

Si bien, la transferencia no consentida de activos es un delito tipificado en el código penal colombiano, a la luz de otras legislaciones de países dentro del derecho comparado, tiene diferentes modalidades, lo cual no permite hacer comparaciones doctrinales ni jurisprudenciales, que incluso a nivel colombiano, son muy pocos los estudios relacionados con este tema, lo cual representa un vacío jurídico para la doctrina del derecho penal en este campo, a excepción de ciertas similitudes con el derecho español y ecuatoriano en esta materia.

Para profundizar en este tema desde la perspectiva dogmática, es menester señalar el pronunciamiento que ha realizado la Corte Suprema de Justicia, Sala de Casación Penal[223] en el caso de recurso de casación interpuesto por la defensora pública de Carlos Arturo Álvarez Trujillo contra la sentencia dictada el 29 de agosto de 2013 por la Sala Penal del Tribunal Superior de Neiva, que confirmó la decisión proferida el 19 de julio del mismo año por el Juzgado Cuarto Penal del Circuito con funciones de conocimiento de esa ciudad, mediante la cual lo condenó en calidad de coautor del concurso de delitos de hurto por medios informáticos y semejantes agravado, concierto para delinquir y falsedad en documento privado.

La corte suprema señala en las consideraciones que:

[223] CORTE SUPREMA DE JUSTICIA SALA DE CASACIÓN PENAL, Magistrado ponente EYDER PATIÑO CABRERA, SP1245-2015,Radicación n° 42.724,(Aprobado Acta No. 44),Bogotá D.C., once (11) de febrero de dos mil quince (2015).

1. El asunto que nos ocupa plantea varias cuestiones a dilucidar que, resueltas afirmativamente, lograrían dar respuesta al problema jurídico de mayor envergadura, consistente en establecer si el delito de hurto por medios informáticos y semejantes admite la figura de la reparación integral, descrita en el artículo 269 del Código Penal y, por ende, si los jueces de instancia incurrieron en la infracción directa de la ley sustancial por falta de aplicación de esa norma como consecuencia de la interpretación errónea del canon 269I ejusdem, al negar dicho derecho punitivo al procesado.

Para definir tal aspecto, la Corte adoptará como metodología de estudio la del conocimiento deductivo, para lo cual, como primer eje temático, examinará los elementos estructurales del aludido tipo penal y sus antecedentes legislativos para, con fundamento en ello, adentrarse en el análisis del bien jurídico protegido y la posibilidad de aplicar el criterio sistemático de interpretación y la analogía en bonam partem.

Finalmente, evaluará si el acusado puede o no ser beneficiario del descuento de pena por reparación integral de que trata el referido precepto 269, previsto para los injustos consagrados en el Título VII.

Con respecto a los antecedentes legislativos del delito de hurto por medios informáticos, la Corte Suprema de Justicia señala:

Debido a la creciente criminalidad en materia informática y a la necesidad de que Colombia alcanzara un nivel normativo similar al de otros países que, de tiempo atrás, venían sancionando infracciones relacionadas con el abuso de los sistemas informáticos y los datos personales –Convenio sobre la ciberdelincuencia de Budapest (2001), adoptado por el Consejo de Europa-, en el Congreso de la República surgió una primera iniciativa –Proyecto de Ley No. 042 de 2007 Cámara224- destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal relativos a la «Violación a la intimidad, reserva e interceptación de comunicaciones»225 y a endurecer las penas del hurto calificado, el daño en bien ajeno, la violación de reserva industrial o comercial y el espionaje, cuando quiera que se ejecuten utilizando medios informáticos o se vulneren las seguridades informáticas de las víctimas.

La exposición de motivos fue expresa en señalar que, de los tres modelos legislativos posibles, a saber, i) ley especial –no integrada al Código Penal-, ii) capítulo especial –incorporado al Estatuto Sustantivo- y iii) modificación de los tipos penales existentes, se optó por el tercero a fin de garantizar la protección de otros bienes jurídicos distintos al de la información que también podían resultar lesionados con actividades relacionadas con la cibercriminalidad.

---

[224] Cuyo ponente fue el doctor GERMÁN VARÓN COTRINO.

[225] Concretamente, la posesión de instrumentos aptos para interceptar comunicaciones privadas, el acceso abusivo a un sistema informático, la violación a la disponibilidad de datos informáticos y sus circunstancias de agravación.

Así lo concibió el legislador:

Cuando se ha optado por una legislación o un capítulo especial que compendie los llamados delitos informáticos se ha partido de la base de la elevación a bien jurídico tutelado el derecho a la información, referida al dato informático (información almacenada, procesada y transmitida a través de sistemas informáticos), o si se quiere, el bien jurídico a salvaguardar es la seguridad informática, teniendo en cuenta que a través de su ataque se pueden vulnerar otros bienes como la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del Estado. Es por eso que algunos doctrinantes catalogan a ese derecho a la información o a la seguridad informática como bien jurídico intermedio que se hace digno de tutela penal, por su propio valor y por el peligro potencial que encierra su quebrantamiento para los demás bienes jurídicos.

Desde ese punto de vista han denominado al delito informático como una acción delictiva en la cual la computadora o los sistemas de procesamiento de datos han estado involucrados como material o como objeto de la misma; y se ha desarrollado el tema alrededor de la triple dimensión de los datos informáticos: confidencialidad, integridad y disponibilidad. Su respeto trae consigo un sentimiento de seguridad y tranquilidad a todos los asociados. De ahí que su transgresión deviene de la afectación de un derecho colectivo o supraindividual que por lo mismo debe ser digno de

protección. Por eso es un bien intermedio para la afectación de derechos individuales.

(…) Nuestra reciente tradición jurídica viene decantándose por la otra modalidad de legislación para este tipo de comportamientos consistente en la modificación de los tipos existentes para adecuarlos a la realidad, manteniendo tales conductas dentro de los capítulos correspondientes sin alterar los bienes jurídicos protegidos, y en esa dirección apunta el presente proyecto pues, como veremos, en gran parte de la iniciativa lo que se busca es agravar conductas actualmente tipificadas, o ampliarles el verbo rector, y solo en algunos casos se pretende tipificar comportamientos no contemplados en la ley penal.

La principal razón para optar por este camino es que son varias las conductas que si bien utilizan medios informáticos para la comisión de los delitos, bien puede asegurarse que no corresponderían a lo que se ha denominado delitos informáticos, sino que son delitos tradicionales remozados con nuevas formas de comisión, pero que ameritan un pronunciamiento expreso de la ley penal para aumentar su castigo dado la alarma social que genera la ruptura de la confianza que se deposita en una actividad cotidiana y necesaria de la vida moderna en la que el derecho a la información ha cobrado vida propia.[226] (Subrayas no originales).

[226] Gaceta del Congreso No. 355 del 30 de julio de 2007, Exposición de Motivos, p. 39-40.

Es así que, luego de la audiencia pública[227], en la que se enfatizó sobre la necesidad de proteger el patrimonio y los sistemas informáticos, se acumularon las dos propuestas legislativas en el Proyecto de Ley No. 042 Cámara, 123 Cámara y Senado[228], dando lugar a la proposición de crear un Título VII Bis al Código Penal, destinado, esencialmente, a la salvaguarda de la información y los datos, tomando como base, para el efecto, las conductas reguladas en el Convenio sobre la Ciberdelincuencia de Budapest y algunas que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, las cuales fueron ubicadas en el capítulo I[229] y un segundo grupo de punibles definidos bajo el rótulo de "*otras infracciones*", concretamente, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva industrial o comercial valiéndose de medios informáticos (capítulo II).

Separaron, pues, en dos conjuntos de normas, los atentados contra la confianza en el tráfico informático y los también lesivos de este bien y otros intereses jurídicos.

---

[227] En la que participaron el ponente de la primera de las iniciativas, algunos congresistas y representantes de los Ministerios del Interior y de Justicia y Relaciones Exteriores, de Incocrédito, la Universidad del Rosario y la Jefatura de Delitos Informáticos de la DIJIN. Gaceta del Congreso No. 455 del 17 de septiembre de 2007.

[228] Gaceta del Congreso No. 528 del 18 de octubre de 2007, Informe de ponencia para primer debate en Cámara.

[229] Las conductas allí consagradas fueron: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación ilícita de datos informáticos o de emisiones electromagnéticas, daño informático, uso de software malicioso (malware), violación de datos personales (hacking), suplantación de sitios web para capturar datos personales (phishing).

En esta oportunidad, explican los Informes de Ponencia para primer y segundo debate en Cámara que, se escogió el sistema legislativo consistente en confeccionar un título adicional para ser incluido en el texto del estatuto punitivo porque si bien, era más técnica la expedición de una ley especial, ella podría perderse «dentro de todo el entramado del ordenamiento jurídico, sin merecer la atención requerida por parte de estudiosos y administradores de Justicia, quienes, pretextando dificultades técnicas, falta de preparación, etc., prefieren dejar en el olvido este tipo de normatividades que terminan por no ser aplicadas o, si lo son, de una manera deficiente»[230] y, asimismo, el modelo adoptado en el proyecto original -042- debido a que contraía «la dificultad de permitir la dispersión de esta problemática a lo largo del articulado lo que le quita fuerza y coherencia a la materia, (…) amén de que (sic) dificulta en extremo la precisión del bien jurídico que se debe proteger en estos casos, esto es, la Protección de la Información y de los Datos»[231].

Una afirmación como la recién transcrita podría sugerir un único valor jurídico a ser protegido: la información y los datos, pero son las mismas ponencias las que precisan frente a los punibles de hurto por medios informáticos y semejantes y transferencia no consentida de activos, que el primero procura «completar las descripciones típicas contenidas en los artículos 239 y siguientes

[230] Gaceta del Congreso No. 528 del 18 de octubre de 2007, Informe de ponencia para primer debate en Cámara, p. 4.

[231] *Ibidem*.

del Código Penal, a las cuales se remite expresamente»[232] y el segundo busca variar la estafa clásica por la figura de la estafa electrónica.

Lo anterior, es una muestra sobre la complejidad de aplicación del derecho penal con respecto al ciberdelito, dentro del cual está la transferencia no consentida de activos.

[232] *Cfr.* Gaceta del Congreso No. 528, Informe de Ponencia para primer debate en Cámara, p. 3.

DISCUSIÓN DE RESULTADOS

Del desarrollo de esta investigación monográfica sobre el Delito Informático en el Marco Jurídico Colombiano y el Derecho Comparado: caso Transferencia No Consentida de Activos, los resultados o hallazgos encontrados al explorar diferentes estudios, artículos de investigación, libros especializados y demás referentes del Estado del arte en el contexto nacional e internacional, se puede afirmar que, la sociedad actual en una economía cada vez más interdependiente y globalizada, en la llamada sociedad del conocimiento, del crecimiento vertiginoso de las tecnologías de la información y la comunicación TIC, el Internet y las redes sociales como medio de comunicación e interacción entre las personas y la sociedad en general, el delito informático y la ciberdelincuencia, se han convertido en uno de los principales problemas para los países, las instituciones, los gobiernos y demás organismos multilaterales que hacen parte de la gobernanza mundial, así lo señalan estudios como el de (Barrios A., 2018; Becerra, Cotino H., García V., Sánchez A., & Torres Á., 2015; Díaz Gómez, 2010; Ferreira, 2018; Ķinis, 2018; Ricardo Posada M., 2017b; Rojas P., 2016).

Si bien existen el Convenio de Budapest como principal referente para combatir el ciberdelito en todas sus modalidades, el avance tecnológico que traspasa la territorialidad y jurisdicción de los países, facilita a los ciberdelincuentes evadir la Ley y el castigo desde el derecho penal, por cuanto la falta de instrumentos jurídico legales de cooperación internacional, de recursos

probatorios, son algunos de los desafíos que enfrentan los países de cara a este gran flagelo de la ciberdelincuencia, tal como lo afirman (Anarte Borrallo, 2007; Gimenez García, 2006; González Rus, 1999; Landecho Velasco & Molina Blázquez, 1996; Lerma, 1999; Marqués Escobar, 2003; Miró L., 2013; Rodríguez, 2000; Rojas Parra, 2016).

Al analizar el ciberdelito desde el derecho comparado, se observa una disparidad entre las diferentes jurisdicciones de los países analizados, por cuanto aquellos que hacen parte de bloques económicos como la Unión Europea, tienen marcos jurídicos más estandarizados, lo cual les permite una mayor cooperación desde lo nacional y lo internacional, según lo afirman (Anjaneyulu & Kishore, 2019; Donalds & Osei-Bryson, 2019; Luong, 2019; Maimon & Louderback, 2019; Miro L., 2012b; Paul Joseph & Norman, 2019; Prokofieva et al., 2019; Sadeghi, 2019; Urban et al., 2019; Yaqoob et al., 2019). Sin embargo, en aquellos países especialmente en vías de desarrollo, como los países latinoamericanos, muchos a pesar de ser invitados a su adhesión al Convenio de Budapest, sus legislaciones no han sido reformadas, lo cual facilita la mayor impunidad frente al ciberdelito, pero además, se carece de herramientas jurídicas y la cooperación que permita establecer un marco común frente a la ciberdelincuencia, así lo sostiene autores como (Ascona Albarrán, 2012; Barrios A., 2018; Becerra et al., 2015; G. Campoli, 2005; G. A. Campoli, 2005; Carrera, 2013; Casanovas, 2012; Cassese, Delmas-Marty, & Pons, 2004; Castro Ospina, 2001, 2007; Catá del Palacio, 2014; Champaud, 1990).

Con respecto a Colombia, en cuanto a la normatividad sobre el ciberdelito y el uso de la información de datos, comercio electrónico, principios y conceptos sobre la sociedad de la información y la organización de las TIC, de la seguridad de las redes de los proveedores y servicios de telecomunicaciones, así como la reforma al código penal, sólo hasta el año 2018, se aprobó la ley 1928 mediante la cual Colombia se adhiere al Convenio de Budapest, por lo tanto, existe aún un vacío jurídico en materia penal, para realizar las modificaciones necesarias en la legislación sustantiva tendiente a construir una política criminal común y una legislación procesal que permita la aplicación de la ley, el combate al ciberdelito desde una perspectiva de cooperación internacional. Antes de la adhesión a este convenio, hay autores que han realizado aportes muy significativos desde el código penal, tales como (Castro Ospina, 2001; Diaz García, 2010; Manjarrés & Jimenez T., 2014; Ojeda P. et al., 2010; Quintero C. & Suárez L., 2012; J. F. Salazar, 2011; Suárez S., 2016; Suárez Sánchez, 2007).

Si bien en Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”, aún existen vacíos jurídicos desde el punto de vista del Código Penal, que se hace necesario analizar y profundizar para lograr incorporar su modernización acorde a

las nuevas modalidades del ciberdelito, dado que, retomando lo anteriormente comentado, la expansión del Internet ha generado una serie de actividades delictivas que afectan a las empresas, las personas y la sociedad en general, especialmente en el caso del sistema financiero frente a la transferencia no consentida de activos, que es un contexto aplicable en España, Ecuador y de alguna manera en Alemania, pero que en otros países no se tiene tipificado este delito bajo este concepto, lo cual también dificulta la posibilidad de establecer un marco común frente a este tipo de delito, especialmente cuando traspasa la jurisdicción territorial. Los aportes realizados por (Grisales P., 2013a; R. Posada M., 2012; Suárez S., 2006, 2016) son de los pocos estudios que se han realizado sobre la transferencia no consentida de activos o cómo estafa informática cuando afecta el bien patrimonial de las personas, las instituciones con las empresas en general.

Si bien, los principales hallazgos constituyen un primer referente sobre el delito informático en Colombia, especialmente en lo referente a la transferencia no consentida de activos, merece mayor atención para futuras investigaciones, especialmente dentro del marco del Convenio de Budapest, que permitirá establecer adecuaciones a la normatividad jurídica desde el código penal y procesal, para ajustarse hacia una cooperación internacional bajo un marco más estandarizados que facilite la penalización del ciberdelito en la sociedad de la información y la globalización en todos sus aspectos.

CONCLUSIONES

Del proceso investigativo y desarrollo de la monografía el Delito Informático en el Marco Jurídico Colombiano y el Derecho Comparado: caso Transferencia No Consentida de Activos, se pueden plantear las siguientes conclusiones:

La globalización y su manifestación en todos los ámbitos de la sociedad actual, junto con el desarrollo de las tecnologías y el Internet, han incrementado de manera paralela el ciberdelito en todas sus formas y variaciones, que afectan a las personas, las empresas, las organizaciones, entidades y Estados de la comunidad internacional, lo cual ha representado un constante desafío para las instituciones multilaterales, en pro de un frente común de cooperación en la implementación de medidas legislativas, jurídicas en derecho penal, para combatir y penalizar el ciberdelito, que por sus características de la comisión y afectación, traspasa las fronteras y las jurisdicciones de los países, presentando situaciones complejas a nivel legislativo, especialmente si las leyes de los países involucrados no están alineadas con las disposiciones emanadas de las convenciones y acuerdos multilaterales.

Si bien desde el convenio sobre cibercriminalidad celebrado en Budapest en el año 2001, se establecieron los lineamientos para reconocer, caracterizar, tipificar y aplicar la normatividad penal al establecer convenios en todas sus modalidades y manifestaciones, muchos países no han protocolizado su adhesión formal dentro del marco jurídico correspondiente, lo cual ha impedido que se genere una acción

común de colaboración entre las naciones, para combatir la ciberdelincuencia, un flagelo que va en aumento y presente grandes riesgos para la seguridad de los países, las instituciones y la sociedad en general.

Si bien Colombia se adhirió mediante Ley 1928 del 24 de julio de 2018 al Convenio de Budapest, cabe señalar que este es un acuerdo común que establece medidas en materia de derecho penal en el marco del Estado de Derecho y los principios de Derechos Humanos. Si bien las medidas contra el cibercrimen ciertamente contribuyen a la seguridad nacional y a la ciberseguridad, mientras que la cooperación internacional contra el cibercrimen basado en este tratado puede contribuir a la confianza entre los Estados para disminuir la escala de incidentes de ciberataques transfronterizos, la Convención de Budapest no es un acuerdo dirigido a incorporar una dimensión político-militar de las relaciones internacionales y desde este perspectiva, no es un tratado sobre ciberseguridad.

El Convenio de Budapest sirve como guía y muchos países la han utilizado como "modelo ley " al adecuar la legislación nacional dentro del marco del Convenio. Sin embargo, a diferencia de otras "leyes modelo", es una negociación que adoptó formalmente un acuerdo internacional y, por lo tanto, también un marco legal para la cooperación que se escalable en términos de membresía.

Si bien existe un marco común, el desafío para los países con respecto a la diversidad y complejidad del ciberdelito persiste, más aun si se consciente que

desde el derecho comparado hay muchas diferencias en torno a la tipificación de los delitos y la aplicación de la ley, lo cual redunda en la impunidad, ante la falta de seguimiento y control por la misma actualización y sofisticación de los medios informáticos, que no permiten la identificación, ni ubicación territorial y jurídica de los delitos cometidos. Existe un permanente desafío para los países y la comunidad internacional en torno a establecer estándares universales que tipifiquen los delitos con elementos normativos y penas similares, bajo criterios de cooperación y jurisdicción internacional.

Para el caso colombiano, el país ha avanzado significativamente en torno al fortalecimiento de la normatividad frente al ciberdelito, muestra de ello, es la promulgación de la Ley que adopta el Convenio de Budapest, sin embargo, aún dista con respecto a la comunidad internacional, para identificar, colaborar y definir criterios comunes para la disuasión, castigo y penalización de los diferentes delitos tipificados acorde con el convenio de Budapest, en consonancia con la legislación interna y latinoamericana. La legislación colombiana sobre el delito informático tiene muchas similitudes con respecto a la legislación española, dada su influencia doctrinal en este campo del derecho penal para tipificar el delito.

Con respecto a la estafa informática bajo la modalidad de transferencia no consentida de activos patrimoniales, la atipicidad de dicho delito, junto con la congestión del sistema de justicia del país, la impunidad y la falta de doctrina y aplicación de criterios jurídicos claros desde el punto de vista del derecho penal,

dejan vacíos jurídicos que es necesario desarrollar, especialmente cuando su configuración dista mucho del concepto existente en otros países, donde este delito hace parte de la estafa, hurto o defraudación cibernética, lo cual impide la aplicación de la Ley, especialmente si el delito traspasa fronteras y afecta otras jurisdicciones, con las cuales no hay similitud en torno a la tipificación de dicho delito.

A pesar de las diversas posiciones que sostienen los estudiosos del delito informático y fundamentalmente en relación con la transferencia no consentida de activos, es importante reconocer los aportes generados en esta materia y destacar el avance normativo que ha tenido España, Ecuador y Colombia, en su esfuerzo por establecer tipos penales autónomos que anticipen las nuevas y crecientes formas de causar daño a través de los sistemas de información.

RECOMENDACIONES

Un programa eficaz contra la delincuencia cibernética transnacional requiere de la cooperación legal entre los Estados que para la aplicación de las normas de la legislación común acordadas. Existe un consenso razonablemente amplio entre los Estados con respecto a muchas formas de conducta que deberían ser tratadas como delitos cibernéticos dentro de las fronteras nacionales. Este consenso debe traducirse en un régimen legal en el que todos los Estados que están conectados a Internet prohíban formas de conducta ampliamente consideradas punibles por ser destructivas o impropias. Actualmente queda mucho por hacer para alentar y, tan pronto como sea posible, exigir a los Estados que adopten posiciones comunes para facilitar la cooperación en la investigación, la preservación de la evidencia y la extradición.

Los Estados deben establecer y designar agencias de alcance internacional para tratar asuntos transnacionales y cooperar con sus contrapartes en todo el mundo. Para desarrollar y asegurar la adopción universal de estándares tecnológicos y de políticas para investigar, enjuiciar y disuadir el delito cibernético. Los Estados deben crear una agencia internacional, diseñada para reflejar las necesidades particulares acordes con la naturaleza del mundo cibernético. La cooperación internacional debe incluir un programa efectivo para mejorar las capacidades de los Estados que carecen de los recursos tecnológicos para cooperar en un régimen internacional integral. Estas medidas, aunque de gran alcance en comparación con las políticas actuales, se pueden diseñar para

maximizar la participación y el control del sector privado, para garantizar que la intimidad y otros derechos no se vean afectados y para no perturbar las actividades e intereses de seguridad nacional de los Estados.

Los Estados a través de sus instituciones públicas como la Policía, considerada como uno de los órganos con mayor compromiso en la lucha contra el ciberdelito y la investigación de conductas que constituyen una afectación a bienes jurídicos tutelados a través del uso de los sistemas informáticos y las redes de comunicaciones modernas, deben estudiar o siquiera considerar la creación de un grupo especial de policía cibernética a nivel mundial, que articule esfuerzos y permita la compartimentación de información en tiempo real, tendiente a prevenir y alcanzar efectivos procesos de judicialización frente al delito cibernético.

BIBLIOGRAFÍA

ABU ISSA, Hamzeh, ISMAIL, Mahmoud y AAMAR, Omar. Unauthorized access crime in Jordanian law (comparative study). En: Digital Investigación. 2019/03/01/, 2019. vol. 28, p. 104-111. [Traducción en línea]

ALKAABI, ALI, MOHAY, GEORGE, MCCULLAGH, ADRIAN, CHANTLER, NICHOLAS. Dealing with the Problem of Cybercrime. Springer Berlin Heidelberg, 2011, ps. 1-18 . [Traducción en línea]

ANJANEYULU, M y KISHORE, Asst Prof A Uday. Financial Fraud Detection with Anomaly Feature Detection on credit card. En: International Journal of Scientific Research & Engineering. 2019. vol. 5, no. 3, p. 2395-566X . [Traducción en línea]

AZAD, Dr, NAFIUL MAZID, Kazi y SHARMIN, Syeda. Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law. En: International Journal of New Technology and Research. 05/01, 2017. vol. 3, p. 1-6 . [Traducción en línea]

BARN, R., BARN, B. An ontological representation of a taxonomy for cybercrime. Association for Information Systems, 2016, p. 12-15 . [Traducción en línea]

BARRIOS A., M. Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015. España: Editorial Reus S.A., 2018, p. 9 – 20

BENÍTEZ ORTÚZAR, I. F., “Informática y delito. Aspectos penales relacionados con las nuevas tecnologías”. En: MORILLAS CUEVA, L. y CRUZ BLANCA, M. J., Reforma del Código Penal. Respuestas para una sociedad del siglo XXI, ed.

Dykinson, Madrid, 2009, pp. 111 y ss. [En linea]: http://www.eumed.net/libros-gratis/2014/1397/tecnologia-delito.html#_ftn24

BLYTHE, J. M. y COVENTRY, L. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. En: Computers in Human Behavior. 2018. vol. 87, p. 87-97 . [Traducción en línea]

BROWN, R. y SMITH, R. G. Exploring the relationship between organised crime and volume crime. En: Trends and Issues in Crime and Criminal Justice. 2018, no. 565 Pg. 1-15 . [Traducción en línea]

CAI, T., DU, L., XIN, Y. y CHANG, L. Y. C. Characteristics of cybercrimes: evidence from Chinese judgment documents. En: Police Practice and Research. 2018. vol. 19, no. 6, p. 582-595. [Traducción en línea]

CALDERONI, Francesco The European legal framework on cybercrime: striving for an effective implementation. En: Crime, law. [Traducción en línea]

CLOUGH, J. Principles of Cybercrime. Cambridge University Press, 2015. . [Traducción en línea]

Código Orgánico Integral Penal, del Ecuador 2014 [En línea] https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf [10-11-19]

Contribution to the Second WSIS Action Line C5 Facilitation Meeting. (2007). The Legal Framework on Cybercrime and Law Enforcement in Mexico. P. 1-16 . [Traducción en línea]

CORTE CONSTITUCIONAL, Sentencia C-224/19, Revisión oficiosa de la Ley 1928 de 2018 “Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest”.

DE HERT, Paul, PARLAR, Cihan y SAJFERT, Juraj The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. 2018. vol. 34, no. 2, p. 327-336. . [Traducción en línea]

CORTE SUPREMA DE JUSTICIA SALA DE CASACIÓN PENAL, Magistrado ponente EYDER PATIÑO CABRERA,SP1245-2015,Radicación n° 42.724,(Aprobado Acta No. 44),Bogotá D.C., once (11) de febrero de dos mil quince (2015).

DIAZ G., A. Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos. 2010, p. 175

DÍAZ G., A. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR. 2010, no. 8, p. 169-203

DI PIERO, Constanza. Recensión a MIRÓ LLINARES, F., El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, Universidad de Navarra, Barcelona, Julio de 2013

DÍAZ GÓMEZ, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest. En: Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR. 2010, no. 8, p. 169-203

DONALDS, C. y OSEI-BRYSON, K. M. Toward a cybercrime classification ontology: A knowledge-based approach. En: Computers in Human Behavior. 2019. vol. 92, p. 403-418. . [Traducción en línea]

FARALDO CABANA. Patricia. Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico, p. 104 – 105. En: Revista de Derecho Penal y Criminología, 3.a Época, no. 3 (2010)

FERREIRA, Eduardo. La Convención de Cibercrimen de Budapest y América Latina:Breve guía acerca de su impacto en los derechos y garantías de las personas. Área Digital de la Asociación por los Derechos Civiles (ADC) 2018), p. 1-14.

FERNÁNDEZ CALVO. Rafael. El tratamiento del llamado delito informático en el Proyecto de Ley Orgánica del Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática). En: Informática y Derecho. p.1150

FLORES P., I. Criminalidad informática: aspectos sustantivos y procesales. Madrid-España: Tirant Lo Blanch, 2012, p. 17

FLORES P., I. Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. En: Revista Electrónica de Ciencia Penal y Criminología. 2015. vol. 17, no. 20, p. 1-40

GAMBA, Jacopo. Panorama del derecho informático en América Latina y el Caribe. En: CEPAL - Colección Documentos de proyectos. 2010, p. 1-44

GERRY QC, Felicity, MURASZKIEWICZ, Julia y VAVOULA, Niovi. The role of technology in the fight against human trafficking: Reflections on privacy and data protection concerns. En: Computer Law & Security Review. 2016/04/01/, 2016. vol. 32, no. 2, p. 205-217. . [Traducción en línea]

GONZÁLEZ C., J. Nuevas amenazas a la seguridad nacional: terrorismo, criminalidad organizada y tecnologías de la información y la comunicación. Valencia, SPAIN: Editorial Tirant Lo Blanch, 2013, p. 233

GOODMAN, S.E. y SOFAER, A.D. The Transnational Dimension of Cyber Crime and Terrorism. Hoover Institution Press, 2013, p. 292. . [Traducción en línea]

GRISALES PÉREZ. Giovanni. Hurto por medios informáticos y transferencia no consentida de activos en Colombia. 2014. En: Revista derecho penal n°:48, jul.-sep./2014, págs. 121-189

HILL, J.B. y MARION, N.E. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st. ABC-CLIO, 2016, p.290

HOOPER, Christopher, MARTINI, Ben y CHOO, Kim-Kwang Raymond Cloud computing and its implications for cybercrime investigations in Australia. En:

Computer Law Implementation of the law enforcement function of the state in the field of countering crimes committed using the internet. Springer International Publishing, 2019, vol. 181. 113-120 p. ISSN 21984182 (ISSN). . [Traducción en línea]

KSHETRI, Nir. Cybercrime and Cybersecurity in Latin American and Caribbean Economies. En: Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan UK 2013, p. 135-151. . [Traducción en línea]

KUMAR, A.P. Cyber Law. Mr.Anupa Kumar Patri, 2009, p.109

LEVIN, Avner y GOODRICK, Paul From cybercrime to cyberwar? The international policy shift and its implications for Canada. En: Canadian Foreign Policy Journal. 2013. vol. 19, no. 2, p. 127-143. [Traducción en línea]

LIMA DE LA LUZ. Maria. Delitos electrónicos. En: Criminalia. Academia Mexicana de Ciencias Penales. Edit. Porrúa, No. 1-6, 1984. p. 100

LOADER, B.D. y THOMAS, D. Cybercrime: Security and Surveillance in the Information Age. Taylor & Francis, 2013, p.390

LUONG, Hai Thanh. Cybercrime in Legislative Perspectives: A Comparative Analysis between the Budapest Convention and Vietnam Regulations. En: International Journal of Advanced Research in Computer Science. 2019. vol. 10, no. 3, p. 1. [Traducción en línea]

MAIMON, D. y LOUDERBACK, E. R. Cyber-Dependent Crimes: An Interdisciplinary Review. En: Annual Review of Criminology. 2019. vol. 2, p. 191-216. [Traducción en línea]

MANJARRÉS, B., I. y JIMENEZ T., F. Caracterización de los delitos informáticos en Colombia. En: Revista Pensamiento Americano. 2014. vol. 5, no. 9, p. 71-81

MATA Y MARTÍN, R.M. Delincuencia informática y Derecho Penal, 2001. p. 53

MIRO LL., Fernando. EL CIBERCRIMEN:Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons, 2012.

MIRO LL., F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Revista electrónica de ciencia penal y criminología, 2012, p. 25

MIRO LL., Fernando. Delincuencia asociada al uso de las TIC. FUOC. Fundación para la Universitat Oberta de Catalunya, febrero 2013. CC-BY-NC-ND • PID_00195950

MUGGAH, Robert y NATHAN, Thompson Brazil's Cybercrime Problem. En: Foreign affairs: Latinoamérica. 2015. vol. 17, p.1-7 . [Traducción en línea]

NADARAJAN, Sivakumar. A Comparative Study of Financial Transaction Cards-Credit & Debit Cards. En: International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2017. vol. 2, no. 6, p. 2456-3307. . [Traducción en línea]

NGO, F. y JAISHANKAR, K. Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the

scholarship on cyber crime. En: International Journal of Cyber Criminology. 2017. vol. 11, no. 1, p. 1-9. . [Traducción en línea]

OJEDA P., J., ARIAS F., M., RINCÓN R., F. y DAZA M., L. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. 2010. vol. 11, no. 28, p. 41-66

PAUL JOSEPH, D.,NORMAN, J. An analysis of digital forensics in cyber security. Springer Verlag, 2019, Vol 815, pp. 701-708. . [Traducción en línea]

POLAŃSKI, Paul Przemysław. Cyberspace: A new branch of international customary law? En: Computer Law & Security Review. 2017/06/01/, 2017. vol. 33, no. 3, p. 371-381. . [Traducción en línea]

POSADA M., Ricardo. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. En: Nuevo Foro Penal. 2017. vol. 13, no. 88, p. 72-112

PRADILLO, Juan Carlos Ortiz Fighting against cybercrime in Europe: the admissibility of remote searches in Spain. En: Eur. J. Crime Crim. L.Crim. Just. 2011. vol. 19, p. 363. . [Traducción en línea]

PROKOFIEVA, E.,MAZUR, S.,CHERVONNYKH, E.,ZHURAVLEV, R. Internet as a crime zone: Criminalistic and criminological aspects.. Springer International Publishing, 2019, Vol. 181 Pgs. 105-112. . [Traducción en línea]

RAHARJO, A.,SAEFUDIN, Y.,FIDIYANI, R. The influence of technology determinism in forming criminal act of legislation . EDP Sciences, Vol. 73 Pgs. 23-45. . [Traducción en línea]

REEP-VAN DEN BERGH, C. M. M. y JUNGER, M. Victims of cybercrime in Europe: a review of victim surveys. En: Crime Science. 2018. vol. 7, no. 1 p. 1-7 . . [Traducción en línea]

REICH, Pauline C, BRILL, Alan E, BALDWIN, Fletcher N y MUNRO, Robert John. Cybercrime & Security. West Publications, 2011, p. 245. . [Traducción en línea]

ROJAS PARRA, Jaime Hernán. Análisis de la penalización del cibercrimen en países de habla hispana. En: Revista Logos, Ciencia & Tecnología. 2016. vol. 8, no. 1, p. 220-231

ROMEO C., Carlos María. De los delitos informáticos al cibercrimen: En Universitas vitae homenaje a Ruperto Núñez Barbero. Ediciones Universidad de Salamanca, 2014, p. 655

SADEGHI, S. H. Pathology of learning in cyber space: Concepts, structures and processes. Springer International Publishing.2019, Vol. 156, pp 1-112. . [Traducción en línea]

SALAZAR, Juan Fernando. Situación normativa de la Sociedad de la Información en Colombia. En: Criterio Jurídico. 2011. vol. 9, no. 1, p. 89-103

Security Review. 2013. vol. 29, no. 2, p. 152-163

SINGH, S. K., RASTOGI, N. Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study. Institute of Electrical and Electronics Engineers Inc. 2018, p. 18-23. . [Traducción en línea]

SMITH, G. S. Management models for international cybercrime. En: Journal of Financial Crime. 2015. vol. 22, no. 1, p. 104-125. . [Traducción en línea]

SOBRINO HEREDIA, José Manuel y SÁNCHEZ GÓMEZ, Fernando J. Retos del derecho ante las nuevas amenazas. Madrid, ES: Dykinson, 2014. p. 400

STANCU, Adriana Iuliana Evolution Of The International Regulations Regarding Cybercrime. En: Public Administration Regional Studies. 2016. vol. 18, no. 2, p. 72-79. . [Traducción en línea]

SUÁREZ S., Alberto. La Estafa Informática. En: Derecho Penal y Criminología. 2006. vol. 27, p. 195

SUÁREZ S., A. Autoría., 3.ª ed. Universidad Externado de Colombia. 2007. p. 248

SUÁREZ S., A. La Estafa Informática. Bogotá: Grupo Editorial Ibañez, 2015, p. 67 - 71, 195 – 197

SUÁREZ S., A. Manual de Delito Informático en Colombia. Análisis dogmático de Ley 1273 de 2009. Bogotá: Universidad Externado de Colombia, 2016. p. 339, 393 - 394, 436 y ss

TÉLLEZ VALDÉS. Julio. Derecho informático 3ª Edición. McGraw-Hill Interamericana Editores S.A. DE C.V. México. 2004. p. 163

TORRES BERNAL, C.A. Metodología de la investigación: para administración, economía, humanidades y ciencias sociales. Pearson Educación, 2006. Pg. 58

TWENEBOAH-KODUA, S., ATSU, F. y BUCHANAN, W. Impact of cyberattacks on stock performance: a comparative study. En: Information and Computer Security. 2018. vol. 26, no. 5, p. 637-652. . [Traducción en línea]

URBAN, V.,KNIAZHEV, V.,MAYDYKOV, A.,YEMELYANOVA, E.. Implementation of the law enforcement function of the state in the field of countering crimes committed using the internet. Studies in Systems, Decision and Control. Springer International Publishing, 2019. Vol. 181, pgs. 113-120. . [Traducción en línea]

VARGAS, J.,BAHNSEN, A. C.,VILLEGAS, S.,INGEVALDSON, D. Knowing your enemies: Leveraging data analysis to expose phishing patterns against a major US financial institution. eCrime Researchers Summit, eCrime. Vol. 2016-June, Pag. 52-61. . [Traducción en línea]

VELASCO, CRISTOS. The Legal Framework on Cybercrime and Law Enforcement in Mexico. Contribution to the Second WSIS Action Line C5 Facilitation Meeting, 2007, pp. 1-16. . [Traducción en línea]

WINMILL, B Lynn, METCALF, David L y BAND, Michael E Cybercrime: Issues and challenges in the United States. En: Digital Evidence Elec. Signature L. Rev. 2010. vol. 7, p. 19. . [Traducción en línea]

YAQOOB, I., HASHEM, I. A. T., AHMED, A., KAZMI, S. M. A. y HONG, C. S. Internet of things forensics: Recent advances, taxonomy, requirements, and open

challenges. En: Future Generation Computer Systems. 2019. vol. 92, p. 265-275. . [Traducción en línea]

ZICCARDI, Giovanni. Cybercrime and jurisdiction in Italy en Informatica giuridica. . En: Privacy, sicurezza informatica, computer forensics e investigazioni digitali. 2012, p. 324. . [Traducción en línea]

ZÚÑIGA, Rodrigo y LONDOÑO, Fernando. Cybercrime and jurisdiction in Chile. En: Cybercrime Jurisdiction: A Global Survey. 2006, p. 141-155. . [Traducción en línea]