¿CÓMO ESTÁ ESTABLECIDO EL HURTO INFORMÁTICO EN COLOMBIA A PARTIR DE LA LEY 1273 DE 2009?

DELITOS E INFORMÁTICA

Andrés Felipe Espejo Valencia

Derecho, Facultad De Derecho Y Ciencias Políticas Y Sociales

Universidad La Gran Colombia

Bogotá, D. C.

2023

¿Cómo está establecido el hurto informático en Colombia a partir de la ley 1273 de 2009

Delitos e informática

Trabajo de Grado presentado como requisito para optar al título de Abogado

Andrés Felipe Espejo Valencia

Director: Henry Torres Vásquez

Derecho: Facultad De Derecho y Ciencias Políticas y Sociales

Universidad La Gran Colombia

Bogotá, D. C.

2023

Dedicatoria

Dedico este trabajo a Dios y a la Santísima Virgen María, guías de mi vida y conocimiento para llevar a cabo todas mis metas;

A mis abuelos que, a pesar de mis dificultades médicas, nunca me abandonaron y quisieron que siempre permaneciera a su lado;

A mis padres por ser quienes me inculcaron la disciplina como clave del éxito, y en especial a mi señora madre que pese a su partida estaría muy orgullosa de mí.

Por último, a los doctores Fabián Sebastián Ardila Torres, Adrián Danilo Ardila Torres y Marcela Ardila por contribuir a mi formación ética y profesional.

Agradecimientos

A la Universidad La Gran Colombia por darme la formación académica que me permitió proyectarme en el futuro como abogado egresado de tan prestigiosa institución; a mis compañeros de grupo quienes me brindaron su apoyo incondicional; a la señora Omaira Espejo Olaya (tía), quien asumió mi cuidado desde la partida de mi madre Beatriz Elena Valencia, y por último a los abogados Yurany Pineda Hernández y Fabián Sebastián Ardila, gerente general del Grupo Jurídico Ardila por ser parte de su equipo de trabajo.

Tabla de contenido

Lista de figuras

Resumen

Los delitos informáticos tienen su origen desde el final de la Segunda Guerra Mundial, en 1945; a partir de entonces, la sociedad iba a enfrentar un gran cambio que estaba relacionado con el concepto de la información. Por ello, con el nacimiento del Internet como instrumento vital para buscar información en los años sesenta, se descubre también una manera delictiva que permite acceder a diferente información y a datos personales de otros. Esta nueva modalidad delictiva se definirá como delitos informáticos. El Congreso de la República promulgó la Ley 1273 de 2009.

Por medio de esta se realizó una modificación en el código penal, en el que se creó un nuevo bien jurídico que fue tutelado para proteger los datos y la información, con el fin de que se conserven integralmente los sistemas que utilizan las Tecnologías de la Información y la Comunicación (en adelante, TIC), además de contener otras disposiciones (Congreso de la República, 2009).

Esta ley constituye un avance en la legislación colombiana porque se tipificaron y penalizaron los delitos que atenten a la información y los datos, que constituyen un bien jurídico. En este trabajo se examina detenidamente dicha ley, con el fin determinar si esos delitos que se cometieron con la utilización de las TIC están vigentes y si con el avance vertiginoso de estas se han incrementado y han aparecido nuevos delitos que no se tipifican en esta norma.

Se destaca que para el desarrollo del presente trabajo la metodología que se utilizó fue la siguiente: revisión de textos que traten de ciberdelitos, específicamente de hurto informático, revisar el incremento de estos delitos durante los dos últimos años, considerando la normatividad nacional e internacional al respecto. Asimismo, se analizó la normatividad colombiana vigente

en lo referente a delitos informáticos y se indagó por los delitos de este tipo más comunes en el país.

Palabras claves: delitos informáticos, tecnología, informática, Internet, hurto.

Abstract

Computer crimes have their origin since the end of World War II, in 1945; From then on, society was going to face a great change that was related to the concept of information. For this reason, with the birth of the Internet as a vital instrument to search for information in the sixties, a criminal way was also discovered that allows access to different information and personal data of others. This new criminal modality will be defined as computer crimes. The Congress of the Republic enacted Law 1273 of 2009.

Through this, a modification was made in the penal code, in which a new legal right was created that was protected and called "information and data protection" the systems that use the Technologies are preserved in an integral way. of Information and Communication (hereinafter, ICT), in addition to containing other provisions (Congress of the Republic, 2009).

This law constitutes an advance in Colombian legislation because crimes that violate information and data, which constitute a legal right, were typified, and penalized. In this work, said law is carefully examined, to determine if these crimes committed through the use of ICTs are in force and if with the dizzying progress of these they have increased, and new crimes have appeared that are not typified in this norm.

It should be noted that for the development of this work, the methodology that was reduced was the following: review of texts that deal with cybercrime, specifically computer theft, review the increase in these during crimes in the last two years, considering national and international regulations at respect. In addition, the current Colombian regulations regarding computer science were analyzed and the most common crimes of this type in the country were investigated.

Keywords: Computer crimes, Technology, Computing, Internet, Theft.

1. Introducción

Los avances científicos y tecnológicos han proporcionado una serie de beneficios que han contribuido a mejorar la calidad de vida a nivel social y la han ido cambiando de forma continua. Las nuevas tecnologías facilitan la cotidianidad de los seres humanos porque permiten desarrollar trabajos con menos esfuerzos, hacen posible la creación de máquinas que agilizan la productividad, mejoran la economía, proporcionan mayor y mejor comunicación, y permiten que un gran número de personas estén conectadas entre ellas. Asimismo, posibilitan la inclusión de más personas al sistema educativo, entre otros aspectos.

La Cuarta Revolución Industrial o Industria 4.0 de acuerdo con el MINTIC (2019), integra el software inteligente y los sensores con las tecnologías de procesamiento de datos, el internet de los servicios, el cómputo móvil, el internet de las cosas, la *big data*, el cómputo de la nube y la inteligencia artificial, las cuales tienen gran impacto en la sociedad actual. Esto ha generado cambios a nivel económico, político, social y cultural, por lo que se afirma que el desarrollo de la Industria 4.0 influye contundentemente en la sociedad actual y presenta manifestaciones tanto negativas como positivas.

En cuanto a los aspectos negativos para la sociedad, se puede afirmar que el implementar las TIC en las empresas ha ido reemplazando la mano de obra y ha traído como consecuencia el aumento del desempleo. Además, la dificultad de los usuarios para adaptarse a los avances acelerados de las tecnologías puede causar impactos negativos. Adicionalmente, las formas de comunicarse y relacionarse de las personas por medio de dispositivos como el celular o el computador llevan al aislamiento y la pérdida de las relaciones interpersonales. Asimismo, la suplantación y el hurto de datos personales afecta la integridad personal y la privacidad. En consecuencia, el uso de los sistemas informáticos y las nuevas tecnologías de la información y de

las comunicaciones pueden tener un impacto negativo en la sociedad si no son utilizados con ética y conforme a lo reglamentado por la ley.

Por ello, esta investigación se realiza con la finalidad de examinar cómo está establecido el hurto informático en Colombia a partir de la Ley 1273 de 2009; asimismo, poner en conocimiento cómo se afectan la información y los datos personales por intermedio de los delitos informáticos. Teniendo en cuenta que las nuevas tecnologías han producido cambios en los ámbitos políticos, económicos y jurídicos, desde el marco jurídico se establecieron políticas y normatividades para que los usuarios que acceden a Internet y a los datos tengan acceso seguro a las distintas plataformas tecnológicas conformando una comunidad en línea.

Con base en la afirmación anterior, desde lo penal, se persigue y castiga con una pena ejemplar a todas aquellas personas que cometan estas conductas que atenten contra el uso adecuado de medios informáticos en adhesión con las TIC, pues se afecta la honra, la intimidad, el buen nombre y la privacidad de la ciudadanía colombiana y demás personas que residen en el territorio nacional.

Esta investigación es de tipo descriptiva. La metodología que se siguió fue la siguiente: se leyeron y utilizaron trabajos de investigación como referencia sobre delitos informáticos, también se revisaron algunas leyes en especial la Ley 1273 de 2009, que tomó como referencia la legislación internacional contenida en el convenio de Budapest. Se revisaron las estadísticas sobre delitos informáticos y se tuvo en cuenta su clasificación.

Se busca analizar el avance de los delitos informáticos de cara al marco legislativo internacional actual y a la Ley 1273 de 2009 de Colombia, con el fin de corroborar si se encuentran vigentes los delitos que se contemplan en esta ley. Asimismo, se hace referencia a las modalidades de delitos en el área informática en Colombia y se examinan las medidas de seguridad informática

en el país y las consecuencias penales para quienes quebrantan estas normas. Para lograr estos objetivos se revisaron trabajos sobre el delito informático, los reportes de la Policía Nacional y la normatividad nacional e internacional.

2. Justificación

El auge de las TIC ha cambiado la vida moderna. Esta nueva realidad ha hecho que surjan delitos informáticos, que cada día se hacen más complejos con el rápido avance de la tecnología y las ciencias. Cada vez son más personas las que tienen acceso a internet y a medios similares de comunicación e información, por lo que es necesario conocer y tener presente la seguridad informática.

El cibercrimen crece velozmente por ello es fundamental estar informados y entrenados para proteger tanto la vida financiera como la personal y familiar. La información y proteger los datos empresariales como personales es responsabilidad de los usuarios y del Estado. Este trabajo de grado se realiza con el fin de determinar cómo está establecido el hurto informático en el país a partir de la Ley 1273 de 2009, y desde la legislación internacional mediante el convenio de Budapest que está vigente desde el primero de Julio del año 2004.

Este convenio da origen a la Ley 1273 de 2009, y desde la doctrina penal se crea el bien jurídico que se tutela para la protección información y de los datos, que consiste en plantear que el acceso a la tecnología es un derecho, y también que es una obligación de las autoridades competentes salvaguardar y preservar la información y la disponibilidad de los datos personales y de las empresas, por medio de la ciberseguridad.

La interdisciplinariedad que se genera entre el campo jurídico y el de los sistemas y las TIC trae como resultado la tipificación y penalización de las diferentes modalidades de delitos cibernéticos, que deben ser conocidos y analizados tanto por los juristas como por los ciudadanos en general para estar conscientes de la vulnerabilidad a la que están expuestos desde el momento mismo en el que tienen acceso a un computador o consultan las páginas de internet.

3. Objetivos

3.1 Objetivo general

Determinar cómo está establecido el hurto informático en Colombia a partir de la Ley 1273 de 2009.

3.2 Objetivos específicos

- Definir qué es el medio informático y las potenciales modalidades de delitos informáticos en Colombia.
- Establecer cuáles son las medidas de seguridad informática en Colombia y cuáles son las consecuencias para quienes quebrantan estas normas que buscan contrarrestar el hurto informático.
- Analizar el avance en materia de delitos informáticos de cara al marco legislativo internacional actual y a la Ley 1273 de 2009 de Colombia con el fin de corroborar si se encuentran vigentes, dada la vertiginosa evolución de las TIC.

4. Marco conceptual

Los avances que se produjeron en las telecomunicaciones y la informática permitieron el desarrollo de las TIC. La información está al alcance de todos en cualquier lugar y momento; también el almacenamiento de los datos a gran escala y, en general, las actividades empresariales y bancarias se pueden realizar virtualmente. Estos avances, que son muy positivos en la vida moderna, traen consigo la aparición de delitos informáticos.

Desde el marco legal, existe en Colombia la Ley 1273 de 2009 que tipifica los delitos y penaliza económicamente o con cárcel a quienes incurran en estas conductas punibles. Según Ojeda-Pérez et al (2010), los delitos informáticos se clasifican en tres grupos: delitos informáticos con finalidades económicas, delitos informáticos con connotaciones sociales, y delitos ideológicos o políticos. En este trabajo se tiene en cuenta los delitos informáticos del primer grupo, principalmente.

Actualmente, en Colombia se cometen muchos fraudes con el uso del internet, las estadísticas muestran que estas acciones van en ascenso al mismo tiempo que los avances tecnológicos, y quienes cometen estos delitos generalmente son personas con conocimientos en sistemas informáticos.

Definir qué son los delitos informáticos no es una tarea fácil, de acuerdo con Hernández (2009), tampoco en sencillo conceptualizar las conductas que se asocian a este delito, además, en la doctrina no hay un concepto unitario que defina este concepto, se ha debatido por varios años si es correcto denominar esta categoría como delito informático o si se deben usar expresiones para definir la realidad que carece de un matiz jurídico-positivo, y que se refieran a categorías de tipo criminológico, por ello, las expresiones de delincuencia informática, delitos o crímenes

informáticos, no se toman como concepto sino como la realidad de unas características concretas. A esto se suma el constante cambio con el que evolucionan las TIC y el desarrollo a la par de las conductas delictivas asociadas a estas.

En esta investigación, se definen los delitos informáticos como todas las acciones ilegales que son cometidas mediante el uso del Internet y la informática; en esta tipología de delitos, la mayor parte de las veces es imposible capturar a quien lo comete, pues se realizan de forma rápida, anónima y a distancia.

Ante la creciente inseguridad informática hay que calcular los riesgos y estudiar la vulnerabilidad de los sistemas y las bases de datos. Esto es tarea de la ciberseguridad o seguridad informática, que se define de acuerdo con Costas (2011), como la que asegura que los recursos de los sistemas de información, que contiene programas o material informático de una organización se utilicen de la manera acordada y que el acceso a la información que contienen, así como los cambios que se realizan sea posible solo para las personas que tienen permiso o autorización.

Por medio de la seguridad informática se minimizan los riesgos, que vienen de muchas partes; pueden provenir del ingreso de los datos, del medio que sirve de canal a la información, del hardware desde donde se transmiten y reciben los datos, de los usuarios, entre otros. Por lo anterior, la tarea más importante de la seguridad informática es reducir los riesgos para alcanzar una mayor seguridad en la protección de los sistemas informáticos y la información que se guarda allí.

En Colombia, tanto la Policía Nacional como la fiscalía, así como otros organismos, además de castigar estos delitos investigan sobre el tema y alertan a la ciudadanía sobre los peligros

del cibercrimen. A continuación, se definen algunos términos técnicos con la finalidad de ayudar a comprender los planteamientos que se hacen en esta tesis.

Informática: de acuerdo con Torres-Torres (2022), es la disciplina asociada a la tecnología que tiene como función educar, crear y desarrollar conocimiento a través de los sistemas que se encuentran en las plataformas tecnológicas y demás sistemas computarizados.

Delito informático: como lo afirma Palomá (2012), es toda culpa o quebramiento de la ley, que se ejecuta por medio de una herramienta o medio informático haciendo posible la consecución del delito por medio virtual, o toda conducta que se realiza a través de la web, cuando el sujeto o la persona ingresa a internet, o en varias ocasiones es la persona que, valiéndose de sus conocimientos en informática hurta bajo esta modalidad.

Internet: es la red que se desarrolló bajo el nombre de Arpanet en 1969. Esa red se caracterizó por que tenía como fin compartir información que permitía contrarrestar los ataques de la extinta Unión Soviética, desde cualquier punto del país norteamericano, pero es un sistema por el cual se compartía información con fines académicos, solo a gente privilegiada de la sociedad americana, ya que los ciudadanos del común no podían acceder a ella, pero este sistema informático dio pie al nacimiento de la informática como disciplina..

Ransomware: Es un programa que cifra la información y para poder liberar esa información en términos informáticos se pide una suma de dinero, es un programa malicioso que secuestra los datos almacenados en un ordenador o móvil, por eso el nombre compuesto inicia con “ransom”, que en español significa rescate. (Núñez, 2021)

Software: es un programa compuesto por una secuencia lógica que cumple una función específica para elaborar, soportar o categorizar la información. Los programas que se instalan en cualquier tipo de computadores son plataformas tecnológicas que permiten llevar a cabo determinada función.

Smishing: Es un delito informático que se caracteriza por cometer fraudes bajo la modalidad de mensajes de texto que se envían, desde un teléfono celular o dispositivo móvil, por ejemplo, se envía al teléfono de un usuario información relacionada a que la persona se ha ganado un premio ya sea una lotería o un vehículo (Ventura, 2020).

Tecnología: es el campo que permite explotar la creatividad humana tras el uso y empeño que pone la mente, desarrollando una serie de habilidades que fortalecen sus conocimientos como, por ejemplo, la exploración de los campos de la ciencia, la aritmética, los idiomas, la biología, la informática y la educación, entre otros.

Vishing: según Jiménez & Milagros (2019), esta es una modalidad de estafa informática que se ejecuta a través de la suplantación de identidad mediante una llamada telefónica y que busca obtener información privada de las personas, principalmente la información bancaria.

5. Marco metodológico

El diseño metodológico elaborado para este trabajo incluyó algunos pasos que permiten desarrollar una investigación exploratoria con características descriptivas, las cuales son:

1. Se hizo una búsqueda bibliográfica de varios textos y documentos académicos, como tesis de grado de maestría y pregrado, referentes al tema de delitos informáticos y sus diferentes modalidades, en especial el hurto informático sobre el cual se trabajó más ampliamente.
2. Se revisó y analizó la Ley 1273 de 2009, y demás normatividades asociadas a esta como el convenio o tratado de Budapest, que busca contrarrestar los delitos informáticos desde una perspectiva vista transnacional.
3. Se tuvieron en cuenta los datos publicados por varias entidades como la Asociación Colombiana de Usuarios de Internet, ACUI; el Centro Cibernético Policial, CECIP; el DANE, la Cámara Colombiana de Informática y Telecomunicaciones, entre otros.

A continuación, se describen detalladamente las fases del presente diseño metodológico:

Primero se buscaron las fuentes bibliográficas que trataran sobre el tema y sirvieran de sustento teórico para el presente trabajo. Luego se hizo la lectura cuidadosa de los materiales y se realizó la toma de notas de las fuentes consultadas para la apropiación de los conceptos y su aplicación al marco teórico del trabajo.

Posteriormente, se revisó la normatividad referente a delitos informáticos, como el Código Penal y la Ley 1273 de 2009; en esta ley se revisan de los delitos que atentan contra los datos y la información de las empresas y las personas, lo que en últimas se busca es asegurar las condiciones de seguridad. Asimismo, se revisó el convenio de Budapest, esto implica tener en cuenta el marco transnacional para contrarrestar los delitos informáticos. Las anteriores son las bases jurídicas para

tratar los delitos informáticos en el país, así como el marco legal internacional que busca contrarrestar estos delitos.

Para cumplir con los objetivos trazados dividimos el trabajo en los siguientes temas:

Primero, se conformó un marco teórico el cual representa un soporte para desarrollar la investigación. Luego se trataron los siguientes temas: 1) el medio informático y las modalidades de delitos informáticos en Colombia; 2) la seguridad informática en Colombia y el delito de hurto informático; 3) los delitos informáticos desde el marco legislativo internacional, la Ley 1273 y otras legislaciones; por último, se presentaron los resultados y las conclusiones.

En cuanto al soporte conceptual se tuvo en cuenta a autores como el abogado y docente William Torres Torres especializado en el derecho informático, quien afirma que la informática es la disciplina asociada a la tecnología que tiene como función educar, crear y desarrollar conocimiento a través de los sistemas que se encuentran en las plataformas tecnológicas y demás sistemas computarizados (Torres-Torres, 2022).

Lo que quiere decir que la tecnología tiene la función de educar pero también debe ser una herramienta a la que se le debe dar un uso adecuado, mas no con fines delictivos porque con el avance de la informática y los aspectos tecnológicos el delito no se queda atrás; la delincuencia asocia todo este tipo de elementos para cometer crímenes y los delincuentes conocen la forma de acceder a un sistema y estudiar de manera objetiva como se hurta la información y las debilidades o vulnerabilidades que pueden presentar los usuarios y las empresas.

Otro autor que habla sobre este tema es el abogado penalista de la Universidad del Rosario Majer Nayi Abushihab, quien define el concepto de hurto informático, tema que se debatió con amplitud en este trabajo. En palabras de este autor, el Estado debe proteger a los usuarios porque

el hurto por esta vía se asume desde la postura constitucional, es decir los derechos que tienen los ciudadanos y demás extranjeros que residen en el país a no divulgar la información sin previa autorización, conforme a la ley.

Desde este marco metodológico se desarrolló la investigación que pretende abarcar los delitos informáticos desde la legislación nacional y trasnacional.

6. El medio informático y las modalidades de delitos informáticos en Colombia

6.1 El medio informático

Hace referencia a todo elemento telemático, digital y de acceso a la plataforma en línea de un sistema informático para desarrollar determinada tarea en los computadores, que se puede clasificar en páginas web, correos electrónicos, programas de aplicación, discos duros portables, memorias USB y dispositivos de extracción.

En consecuencia, el medio informático es toda herramienta tecnológica que al ponerla en funcionamiento permite acceder a la información presente en la red. Por consiguiente, este medio está ligado al concepto de las TIC, que según el MINTIC, se conforma por el grupo de herramientas, recursos, programas informáticos, redes, aplicaciones, y medios en lo que se compila, procesa, almacena y transmite información como: imágenes, video, texto, datos y voz. (Congreso de la República, 2009).

Por otra parte, desde el contexto digital en Colombia ACUI, busca promover la socialización, conocimiento, aprovechamiento y buen uso de las TIC principalmente de Internet, en todo el país y promover su importancia como medio de comunicación, información, y educación, ya que es un gran instrumento al servicio del desarrollo social, político y económico.

En el contexto digital en países como México, los medios informáticos son conexos a las TIC. En las sociedades latinoamericanas esto adquiere un gran terreno, según se puede constatar con los datos de la Asociación Mexicana de Internet, en la que se afirma que el país en el año 2006 tenía 20,2 millones de usuarios en la red, sin embargo en el 2018 ya contaban con cuatro veces más de usuarios, hasta alcanzar los 82,7 millones y un 71% de usuarios con más de 6 años.

El grupo etario en el que hay más usuarios se encuentra entre los 25 y los 34 años con un 22%, por su parte el de los 6 a 11 años ocupan el 12%. Los menores de 17 años representan el 26% y los mayores el 74%. Además, se ha evidenciado que un 82% de las personas ingresa a redes sociales cuando ingresa a la red y un 76% se centra en la búsqueda de información.

Por otro lado, de acuerdo con El Tiempo (2022), según el DANE, en su encuesta TIC en los hogares, en Colombia solo el 61,6 % de las viviendas cuenta con conexión a Internet. Bogotá es el territorio con el mayor reporte de conectividad con 81 %, seguido de Santander con el 74 % y, en tercer lugar, el Valle del Cauca con 72,3 %, esta conectividad crece año tras año.

Lo que significa que el uso de las plataformas tecnológicas, las redes sociales y demás formas de conectividad han facilitado y fortalecido la capacidad de acceder a internet, pero han generado la habilidad para delinquir y hacer daño a través del medio informático, tanto en Colombia como en el mundo entero.

6.2 Modalidades de los delitos informáticos en Colombia

Como se ha dicho antes, los avances en las TIC provocan también el surgimiento los delitos informáticos que se convierten en un problema difícil de afrontar, ya que como lo expresa Guarnizo (2020), anteriormente eran cometidos de manera aislada y actualmente han ido evolucionando hacia la conformación de organizaciones internacionales dedicadas al cibercrimen.

El término cibercrimen nació aproximadamente hace veinte años, asociado al fenómeno criminal que involucraba los delitos que se ejecutaban con el uso de las TIC, siendo un método novedoso y poco conocido por la sociedad en general.

Según Ojeda et al. (2010), los delitos informáticos son de tres tipos económicos, políticos o ideológicos y sociales. Los que predominan en Colombia son los delitos informáticos con fines

económicos. Ahora bien, los principales delitos informáticos cometidos en Colombia, entre el 2017-2019 d

e acuerdo con Guarnizo fueron: hurtos informáticos 31.058, acceso abusivo a sistema informático 8.037 casos, violación de datos personales 7.994 casos, la transferencia de activos sin consentimiento 3.425 casos y finalmente, uso de *software* malicioso con un total de 2.387 casos.

En consonancia con lo anterior, se entiende por *hurto por medios informáticos* la acción que realiza una persona que, sin estar facultada para esta operación, obtenga, suministre, exporte, intercambie, envíe, utilice códigos y datos personales que se encuentren en bases o medios como estos para beneficio propio o de terceros. Asimismo, la contravención de *violación de datos personales* consiste en la acción de una determinada persona que se apodera de la identidad de otra sin su autorización con el fin de hacer parecer a la persona suplantada como deudora de una suma considerable de dinero.

Sumado a los anteriores delitos el *acceso abusivo* se lleva a cabo cuando alguien sin autorización o por fuera de un acuerdo, accede a todo el sistema o a una parte de este. Asimismo, *la transferencia no consentida de activos* es la modalidad delictiva en la que se realiza una transferencia contable y automática de cualquier clase de activos o valores; es decir, dinero en cheques o en efectivo, sin autorización ni consentimiento del titular en perjuicio de un tercero que afecte el patrimonio de una persona.

Por último, *el uso de software malicioso* consiste en la acción de robar datos confidenciales de un computador, disminuir gradualmente la velocidad de este e incluso enviar correos electrónicos falsos desde la cuenta del correo electrónico de una persona sin su conocimiento. Los ciberataques con *software malicioso* se reflejan en los diversos reportes de infecciones que

generalmente se propagan por *phishing* o porque los usuarios navegan desprevenidamente en sitios infectados en la web.

En un estudio de la CCIT (2019), se publican datos estadísticos sobre la cibercriminalidad en el país y las técnicas identificadas en el año 2019 al analizar 15.948 casos denunciados por ciudadanos y empresas al Centro Cibernético Policial CECIP.

Sumado a los anteriores datos, el delito informático que más denunciaron los colombianos es el hurto por medios informáticos con 30.058 casos, los delincuentes buscan sustraer el dinero de las cuentas bancarias, por ello, buscan interferir los dispositivos usados en la interacción entre los bancos y los usuarios como, por ejemplo, cuando un usuario usa computadores en sitios públicos para hacer transacciones bancarias.

En segundo lugar, está el delito de violación de datos personales, que cuenta con 8.037 casos, es decir que el robo de identidad es la segunda amenaza para empresas y personas en Colombia.

El tercer delito con más denuncias es el acceso abusivo a los sistemas informáticos con 7.994 casos. El cuarto delito es la transferencia sin consentimiento de activos, el delincuente sustrae dinero o transfiere activos financieros de las personas.

Por otra parte, la CCIT, a través del tanque de análisis TicTac y el programa Safe, elaboró un informe de ciberseguridad en Colombia. El estudio muestra que, en el primer semestre de 2022, los ciberdelitos que se denunciaron al Sistema Penal Oral Acusatorio de la fiscalía registraron un aumento del 8 %, en comparación con el año 2021. Las cifras son las siguientes: 29.778 denuncias en 2022, mientras que en el 2021 se reportaron 27.498 denuncias.

Según el mencionado reporte, estas cifras dan a conocer los distintos tipos de ciberdelitos que presentaron un aumento en el país, estos son: el acceso abusivo 6.407 casos, ubicado en el 46 % con un aumento en el mismo periodo del año anterior, y el hurto informático que alcanzó un aumento del 15% con 11.078 casos registrados.

Este incremento de hurtos por medios informáticos se debe a las numerosas campañas de *sotfware* malicioso o *malware*, unidas a la suplantación de entidades del gobierno; esto hizo que se incrementaran los casos de virus. Un ejemplo, para destacar es la suplantación de una entidad como la Registraduría por medio de correos electrónicos.

Del mismo modo, el estudio mostró que los virus en los sistemas informáticos con programas maliciosos para cifrar la información, denominados como *ransomware*, siguen siendo afectados por las acciones de las empresas y pueden incluso tener como consecuencia la suspensión o no continuidad de los negocios.

Por otra parte, también hubo reducción de los distintos tipos de cibercrimen: se redujeron durante el primer semestre la suplantación de sitios web y la violación de datos personales, en las que se captaban datos personales y se usaban softwares maliciosos.

Las autoridades encargadas de la ciberseguridad recomiendan estar alertas porque siguen existiendo modalidades como el *ransomware* o secuestro de información, que se está volviendo más común en Colombia.

Las ciudades con mayores registros de ciberataque en el primer semestre de 2022 fueron Bogotá, Cali, Bucaramanga, Medellín y Barranquilla, en estas ciudades se presentaron más del 70 % de las denuncias, esto debido al incremento de usuarios y al uso de internet en plataformas de *e-commerce* y banca virtual, según el informe de la CCIT (Portafolio, 2022).

Lo anterior indica que el tipo de cibercrimen que predomina es el debido a que es una forma rápida por robar dinero de las víctimas. De otro lado, según el reporte de Ccit, la suplantación de los CEO es otra modalidad que se ha empezado a popularizar en la que se hacen pasar por los gerentes o CEO. A través de técnicas en las que se roba información enviando enlaces con formularios fraudulentos o llamadas telefónicas y se obtiene información de procesos comerciales y productivos de las empresas (Portafolio, 2022).

Se deben implementar continuos controles en los que se autoricen y aprueben los pagos de nómina o pago de facturas a proveedores porque estas actividades son aprovechadas por los cibercriminales para cometer fraudes, según este informe.

En relación con lo anterior, el FBI afirma que el fraude BEC en el mundo durante 2021 alcanzó una alta cifra (USD 2,4 billones), y se constituye en el delito de mayor afectación económica para las empresas y personas en el mundo.

El Estado colombiano debe invertir e incrementar las políticas seguridad informática para reducir estos delitos informáticos. Debe capacitar a las personas para evitar que se presenten estas actividades ilícitas, así mismo los ciudadanos deben denunciar estos hechos ante las autoridades competentes.

Según los hechos mencionados anteriormente, se puede corroborar que las modalidades de delitos citados están contemplados en la Ley 1273 de 2009, lo que cambian son las técnicas. Esto quiere decir que dicha Ley tiene plena vigencia.

7. Seguridad informática en Colombia y delito de hurto informático

7.1 Seguridad informática

La seguridad informática es la rama de la computación que cumple la función para proteger los sistemas de amenazas internas o externas, estas últimas vienen de un entorno en el que se encuentran sistemas como virus, robos y ataques informáticos, entre otros, la amenaza interna por su parte es todo riesgo informático que nace dentro de la misma organización o entidad.

Según Hernández (2009), la seguridad informática es un bien jurídico a tutelar que puede ser objeto de ataque con conductas ejecutadas en diferentes modalidades de cibercrimen, este es un bien y protegerlo evita que se generen lesiones a los bienes jurídicos individuales, como la información y los datos personales, que corren peligro por las conductas que atentan contra las redes y la seguridad de los sistemas.

En lo que concierne al concepto de seguridad informática, es necesario mencionar los *insiders* (término inglés) que significa "el que está dentro", se refiere a toda persona o grupo de individuos que manejan la información confidencial de una organización, o entidad empresarial. Así, los *insiders* son en el tipo de empleados con acceso legal a los activos de la empresa, tanto actuales como retirados, que pueden ser contratistas, socios comerciales o proveedores. Por lo tanto, este tipo de personas tiene gran incidencia en la seguridad informática.

Otro concepto de seguridad informática se refiere a todo tipo de bases tecnológicas que conforman la ciencia de la informática, una de las bases que componen esta definición es el concepto de seguridad, entendiendo a este de acuerdo con Romero (2018), como el estado en el que hay bienestar y no existen riesgos por la confianza sobre algo o alguien, la seguridad se toma desde lo disciplinario ya que se puede definir como una ciencia interdisciplinaria que evalúa y

gestiona los riesgos que tienen las personas, los animales o los bienes, por ende, existen países en los que la seguridad se concibe como un tema nacional, aunque este depende de la seguridad y de sus tipos como, la seguridad en el ambiente, en la economía, en lo sanitario, y en la mayoría de las naciones al analizar esta categoría se refiere a la seguridad de las personas, evitar un estado de riesgo, un robo, un daño material o físico.

Tal como se argumentó anteriormente, la seguridad informática busca la prevención de los riesgos que se puedan presentar en materia de infraestructura tecnológica e informática, para poder prevenir y evitar que ocurra todo tipo de amenazas que atenten contra el bienestar de una persona o una entidad empresarial en términos de información.

Por consiguiente, la seguridad informática debe tener en cuenta tres aspectos principales que son: la infraestructura, la información y los usuarios. Los usuarios son los puntos de partida los sujetos a los que se les puede vulnerar la información, pues con los datos que se extraiga de manera ilícita los ciberdelincuentes pueden hacer uso indebido de la información, debido a que los usuarios cometen errores que pueden ser inevitables, por eso cuando ocurre algún tipo de vulneración a la seguridad informática es precisamente a causa de un error humano, por ejemplo se reveló claves de acceso a sistemas informáticos a personas no autorizadas u ocurre algún accidente en el entorno de trabajo que puede ocasionar daños irreparables a los sistemas como a la función del usuario.

La información es el elemento más valioso que conforma todo lo relacionado con los usuarios y las entidades de tipo público, privado, educativo y del sector salud, pues allí reposan los datos de las personas a las cuales se les puede vulnerar la información, información que se debe proteger y salvaguardar.

Por último, la infraestructura se convierte en uno de los medios que tiene mayor control, eso no quiere decir que no se exista un riesgo, pues depende del proceso que se maneje en términos de información. Por ejemplo, son también problemas en parámetros de seguridad de la información el acceso sin autorización, la suplantación personal, los daños como, robo de hardware, incendios, inundaciones o desastres naturales que generen daño físico al sistema informático de la compañía.

Es importante aclarar que la seguridad informática debe ser auténtica, es decir debe existir un proceso en el que se confirme que existe un acierto, no siempre consiste en identificar un usuario, se requiere identificar si los cambios de datos se procesan, pues no siempre los usuarios necesitan de un estudio de autenticidad en la información, por ejemplo, los requiere un dispositivo, una persona o un sistema.

La autenticación es un método de identificación en el mundo de la computación, solo que no se aplica a la contraseña del correo electrónico o de una red social; un ejemplo, las credenciales que se generan al hacer una votación en un país es un método autenticado, un ejemplo adicional se da al ingresar a un país y presentar un documento de identificación como el pasaporte o la visa

Otro método para autenticar es pedir un número de ID en los trabajos para que los empleados puedan tener acceso a determinadas áreas o para generar un registro de cada movimiento y poderlos validar de ser necesario, estos se pueden crear con las huellas, la voz. Se destaca que para la calidad informática se debe contar con mecanismos que prevengan los problemas en esta área como pago de seguro contra accidentes o daños por algún tiempo.

7.1.1 Seguridad informática en Colombia

Actualmente se usan todo tipo de dispositivos como computadores, celulares, para acceder a la información personal, empresarial o de interés general y no se toman las medidas para evitar riesgos en el manejo de estos datos. En relación con esto surge el término de la ciberseguridad o seguridad informática, que es toda práctica para defender los computadores, dispositivos, sistemas y redes de los ataques que causan graves daños a los usuarios. La ciberseguridad también es conocida como seguridad de las TIC y es aplicada en varios entornos, como los negocios y la informática relacionada con los celulares.

La seguridad informática en Colombia está contemplada por la Ley 1273 de 2009; esta ley es la encargada de regular los crímenes informáticos, mediante el código penal en los artículos 269-A y siguientes, en donde se establece que estos delitos son los que que ejecuta un tercero, actuando detrás de un sistema o medio informático, de manera anónima. También, mediante el delito de hurto informático se obstaculiza el buen funcionamiento o el acceso regular a un sistema informático.

Toda persona o empresa debe buscar mecanismos para proteger los datos y evitar riesgos respecto a la información que maneja. Los riesgos informáticos hacen referencia a las amenazas y vulnerabilidades que generan afectaciones en todos los niveles a las empresas y personas, por lo tanto, las consecuencias pueden tener un grave alcance en relación con los datos que se debe proteger siendo confidencial, la cual debe ser salvaguardada mediante estrategias que eviten la sustracción de información de manera fraudulenta.

En relación con lo anterior, Colombia cuenta con medidas para que las personas y las empresas se actualicen sobre los mecanismos que evitan situaciones en el robo de los datos.

También cuenta con diferentes herramientas para enfrentar estas situaciones, como: medidas de protección, cartillas, plataformas virtuales, leyes, casos reales, cursos que capaciten a las personas, entre otras. El Código Penal colombiano ha establecido sanciones a los que cometen delitos informáticos que atentan contra las personas y las entidades, esto permite controlar y disminuir dichos casos.

Las principales sanciones que establece este Código son de tipo penal y económico; así por ejemplo, se enviarán a la cárcel a los individuos que cometan estas infracciones por un tiempo de 48 a 96 meses y pagarán una multa de 100 a 1000 Salarios Mínimos Mensuales Legales Vigentes, quienes tengan un acceso abusivo a los datos o hurten por medio informático y generen obstáculos en las funciones de la información de un sistema, una base de datos o los sistemas o *software* contables (artículo 269D).

En relación con los delitos informáticos algunas veces son los empleados de una empresa los que intercepten la información y utilicen *software* o programas maliciosos para obtener información importante y usarla en su beneficio propio. Al respecto de esto el código penal señala quienes sin orden judicial capte datos de un sistema o las emisiones electromagnéticas que vienen de un sistema informático podrá incurrir en penas de treinta y seis a setenta y dos meses. (Congreso de la República, 2009).

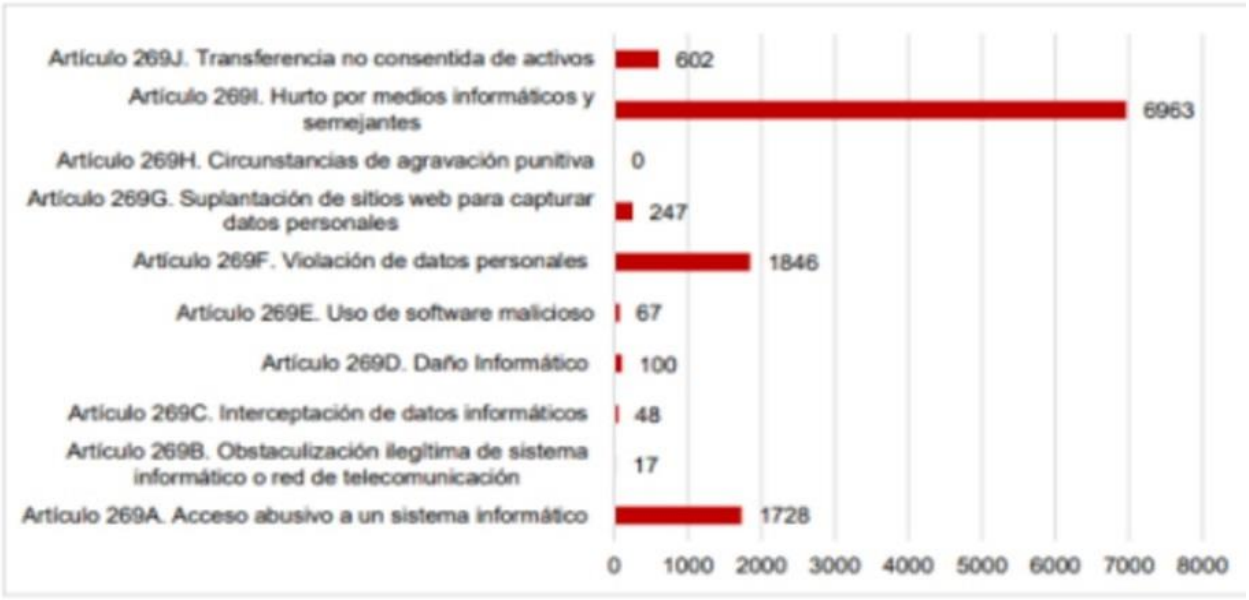
En los casos en el que el uso de sistemas infectados o maliciosos violen los datos personales la ley establece que, si alguien inserta estos sistemas con efectos dañinos puede incurrir en penas de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, tal como se establece en el artículo 269 D de la ley 1273 del 2009.

Debido a este tipo de delitos que se ejecutan por medio telemático y a las sanciones en materia penal que están contempladas en la Ley 1273 de 2009, los usuarios y las empresas han optado por tomar capacitaciones y estudios que van encaminados en materia de seguridad informática y ciberseguridad, desde el año 2020 cuando se produjo el cambio y la evolución tecnológica en la computación y en materia de uso de las TIC, la virtualidad ha generado que el tema de seguridad en infraestructura informática sea una necesidad, pues la tecnología es parte del diario vivir.

A continuación, se presentan algunos datos sobre delitos informáticos en Colombia que abarcan desde el año 2017 al 2020.

Figura 1

Delitos informáticos denunciados en 2017



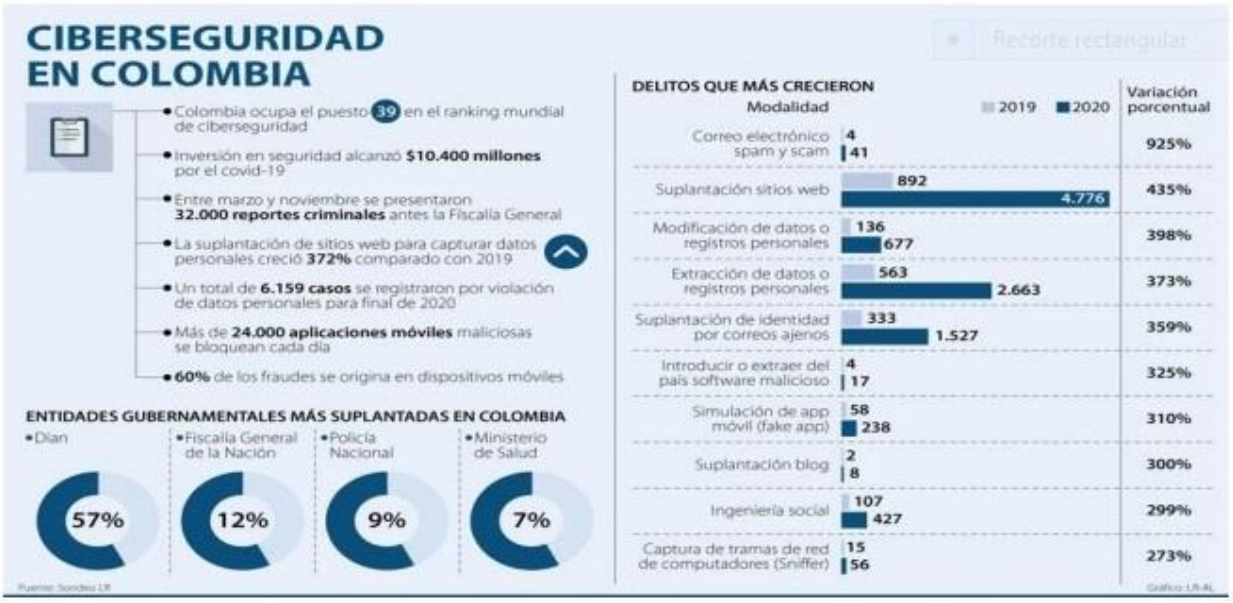
Nota. Tomado de: "Delitos Informáticos en Colombia" por Centro Cibernético Policial, 2017.

En la Figura1 se evidencia el incremento de delitos informáticos denunciados en el 2017, entre los que sobresalen tres clases: *Hurto por medios informáticos* y similares con un total de

6.963 casos, *violación de datos personales* con 1.846 casos y el *acceso abusivo a un sistema informático* con 1.728 casos.

Figura 2

Aumento de la cibercriminalidad en Colombia, 2019-2020



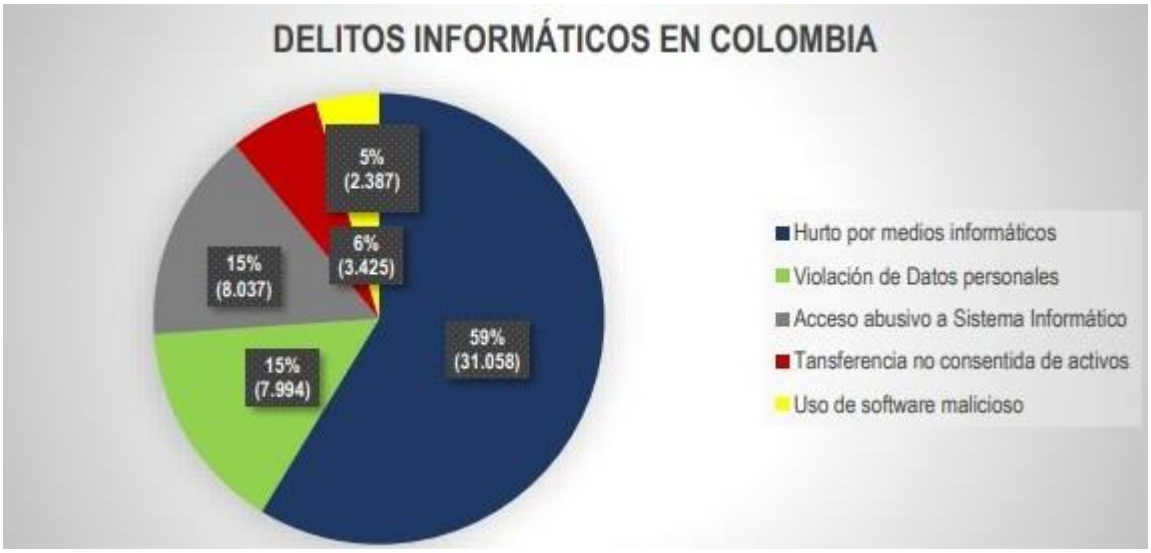
Nota: Ciberseguridad en Colombia. Tomado de "Asuntos legales" (Grafico), Acosta Argote.2021 Recuperado de: https://www.asuntoslegales.com.co/actualidad/ciberdelitos-subieron-37-durante-el-primer-trimestre-de-2020-en-los-peores-meses-de-la-crisis-3126480. CC By 2.0

Nota. Tomado de "Aumento de la Cibercriminalidad en Colombia, 2019-2020" A. Argote 2021.

De acuerdo con la Figura 2, Colombia se ubica en la posición 39 en el ranking mundial de ciberseguridad; debido a que se hizo una gran inversión en seguridad entre 2019 y 2020. Sin embargo, los ciberdelitos que aumentaron en este periodo fueron: suplantación en sitios web, de 892 a 4.776; extracción datos personales, de 563 a 2.663; suplantación de identidad vía correo, de 333 casos a 1.527 casos, y modificación de datos o registros personales, de 136 casos a 677, principalmente. Asimismo, sobresalen en estos datos, las entidades del gobierno más suplantadas en Colombia: la Dian con un porcentaje de 57 %; y con porcentajes más bajos, la Fiscalía con el 12 %, la Policía con 9 % y el MINSALUD con 7 %.

Figura 3

Delitos informáticos en Colombia



Nota. Figura tomada de Guarnizo (2020).

Según Guarnizo (2020), los delitos informáticos de mayor tendencia entre 2019- 2020 son: el hurto por medios informáticos, el acceso abusivo a Sistema informático, el uso de *software* malicioso, la violación de datos personales y la transferencia no consentida de activos.

Para concluir este apartado, se cita un caso de ciberdelincuencia que ocurrió recientemente en Colombia, un grupo anónimo internacional de *hackers* llamado RansomHouse como lo refiere Osorio (2022), realizó un ciberataque a una entidad prestadora de salud. Este grupo dice proteger a los usuarios de las grandes empresas alrededor del mundo que no cuidan su información personal, pero luego hacen un ataque informático a estas para demostrar que pueden robar sus datos privados y extorsionan a las empresas para que paguen o de lo contrario publican o venden los datos. Lo que hace en realidad RansomHouse es robar los datos privados de las empresas para luego pedir

dinero a cambio de no divulgar esos datos. Este ciberataque demuestra que Colombia tiene que robustecer el esquema de ciberseguridad. Hay tendencia al crecimiento de este tipo de delitos en el país, así lo demuestra el Centro Cibernético de la Policía en el que se registraron 11.223 denuncias de ciberataques y en el 2022, de enero a octubre, las denuncias se aumentaron a 54.121.

7.2 Hurto informático

En este apartado se va a tratar ampliamente el hurto informático, por lo cual se comenzará por definir esta modalidad de delito, se dará a conocer quiénes son los sujetos activos y pasivos y como se afecta la información personal.

El delito de hurto informático se define como toda conducta criminal realizada a través de una computadora o un medio informático, con el fin de obtener un resultado de manera ilícita o sin consentimiento de la víctima. Por esta razón, el delito informático es una acción jurídica y culpable, que, para poder ser ejecutada, se emplea el uso de tecnología informática para hurtar la información.

Lo que más se caracteriza en la ejecución de un delito informático es el lugar donde se consumó la conducta: se tendrá como primera evidencia el sitio donde ocurrió el delito, el país, además, a quien correspondía ejecutar el resultado, porque el atentado informático puede ir dirigido en contra de una persona, para hurtar y obtener la información de sus contraseñas, lo cual permitirá acceder a sus cuentas bancarias y sustraer el dinero de manera fraudulenta.

Inclusive para obtener información crediticia laboral o clínica, o también con fines terroristas, lo cual afecta los bienes jurídicos de las personas que residan en el país en donde se

comete la acción de hurtar. Téngase en cuenta el principio de la nacionalidad o personalidad activa que afirma que:

> La ley penal sirve a sus nacionales en donde quieran que se encuentren, cuando se lleven a cabo las conductas punibles. Ahora bien, cuando se trata de un nacional de un Estado que es víctima de una conducta delictiva en el territorio de otro Estado distinto al suyo, se aplica el principio de personalidad pasiva, que significa que la ley penal de su territorio los protege, y perseguirá a quien o quienes hayan ocasionado afectaciones a sus bienes jurídicos. (Forero et al., 2019, p. 22)

Por esta razón, esa información no puede bajo ningún pretexto ser objeto de divulgación sin autorización del usuario, ya que eso compromete la identidad de la persona, en términos de integridad moral y física, lo que pone en riesgo no solo al sujeto sino a su familia o las personas allegadas, porque el delincuente informático realiza con todo el rigor un perfilamiento social para obtener conocimiento de las personas o entidades que se atacarán, hurtando la información que requiere.

El objeto es todo aquel elemento informático que afecta plenamente los intereses de los bienes jurídicos tutelados. Además, el hurto informático se asocia directamente al concepto de *computer crime*, el cual:

> Consiste en una denominación genérica y no específica de aquellas infracciones informáticas, en este caso el hurto informático, es decir, contenidos en el campo de la actividad informática contra bienes que sean tangibles o en contra del tratamiento automatizado de datos. (Torres-Torres, 2002, p. 24)

De acuerdo con la afirmación anterior, el computador se convierte en un instrumento para cometer delitos, en especial el hurto informático; esto implica que exista un conocimiento en tecnologías informáticas, principalmente en los sistemas de *software*, por ejemplo, el saber cómo se usa un sistema para acceder al usuario y descubrir la contraseña de la persona u organización de la cual se hurtará la información.

Es aquí donde el delito informático está conexo a todas las actividades criminales que se pueden presentar: hurtar, acceder, extorsionar e intimidar, entre otras, así que la conducta delictiva se realiza en distinto modo, pero en cualquier momento se puede disponer de la información, cuando se requiera.

La información se considera como el grupo de mecanismos que le dan la posibilidad al individuo de retomar y organizar los datos del medio sobre el cual se obtiene conocimiento, con el fin de que el contenido sea estructurado de una manera determinada y así la información se convierta en una guía para concretar un objetivo trazado. Señalan distintos teóricos y académicos que han evaluado la posibilidad de crear una ciber corte penal internacional ante conductas graves como la pornografía infantil, los ciberataques terroristas, los daños a sistemas informáticos y la infraestructura informática, ya que se puede constatar que:

> No bastan las leyes y las regulaciones actuales, pues no resultan suficientes para dar una respuesta eficaz a las problemáticas que surjan tanto de la falta de regulación del ciberespacio como de la creciente actividad para interponer ciertas restricciones, por eso se ha propuesto la creación de un tribunal internacional que tendría la facultad de enjuiciar a las personas individualmente que cometen los delitos cibernéticos más graves de trascendencia e interés global. (Forero et al., 2019, p. 36)

Por tal motivo, la seguridad informática se vulnera por un medio informático que recurre al uso del campo virtual o en línea; por eso, en varios países existen legislaciones que no han aplicado en el delito informático una sanción jurídica adecuada al respecto, pues las penas para estos delitos son de interpretación jurídica y es difícil probar o tener certeza del individuo que hurta a los usuarios.

En concordancia con lo anterior, hay que buscar la forma de crear leyes y normas que regulen el uso de las tecnologías, así como el uso y suministro de equipos y aplicaciones sistematizadas según como corresponda a cada país, pues la tecnología es parte del sistema de gobierno, así que es responsabilidad de los mandatarios proteger la información, salvaguardar los bancos de datos de la ciudadanía y evitar que se cometa el delito de hurto informático, fortaleciendo la seguridad informática como herramienta que prevenga este delito.

Para cumplir con esa labor, se debe involucrar a la ciudadanía, alertándola por medio de estrategias de seguridad digitales, por medio de las cuáles son las personas las que tienen derecho a recibir información de manera oportuna, y asimismo rectificar el contenido en los casos que sea necesario; por ejemplo, en el hurto informático hay que identificar el accionar delictivo que implique el uso indebido de una máquina, con el fin de causar un perjuicio, que genere un beneficio propio o de un tercero.

Por consiguiente, el elemento objetivo dentro del hurto informático es utilizar una máquina en la que se le genera un perjuicio material o moral a alguien, o se utiliza de forma indebida una computadora sin tener la autorización, por ello, el elemento subjetivo debe contar con la intención de culpa o dolo con la que actúa el individuo que comete el hurto informático.

Se puede decir que el hurto informático en el país se desarrolla por el uso tan desmesurado de la tecnología y su llegada a la nación, y por esta razón este delito va en aumento. Por ejemplo, en el departamento de Córdoba entre 2015 y 2016 hubo un incremento considerable del presente delito.

Esto se evidencia de acuerdo con Devia & Martínez (2019), ya que se colocaron 152 denuncias por el hurto informático y similares, de estas, 88 denuncias la victima fue del sexo masculino, por ello, se puede afirmar que un hombre entabla más fácil una conversación con desconocidos que una mujer, ya que el porcentaje de casos en el sexo masculino fue del 57,9%.

No solo en el departamento de Córdoba hubo denuncias contra el delito de hurto informático, sino en muchas regiones durante la pandemia del covid-19 en el país, como se puede evidenciar en la siguiente cita:

> Hubo un aumento del delito del cual se hace mención (hurto informático), según estadísticas en todo Colombia se registró un total de 13.314 hechos relacionados con el delito de hurto informático en el año 2019, y para el año 2020 un total de 17.815 casos, dando a conocer un aumento del 34 % por ciento. En cuanto al primer trimestre del 2021, se registran un total de 5.129 noticias, frente a 3.133 del 2019 y 3.498 del 2020. (Cadena, 2021, p. 19)

Otros datos en relación con el delito informático son los suministrados por el centro cibernético de la Policía Nacional quienes señalan de acuerdo con Cadena (2021), que se presentaron durante los primeros meses, de enero a marzo, de los años 2019, 2020, 2021, un total de 4.732 casos de hurto informático.

Según lo anotado anteriormente, durante los años mencionados, los casos y denuncias criminales que hablan sobre hurto informático demuestra que las personas no cuentan con la suficiente información para prevenir este tipo de ataques, por ejemplo, las personas no invierten en programas informáticos que eviten, desde el punto de vista tecnológico, un hurto informático.

Asimismo, los usuarios deberían tener capacitaciones virtuales o presenciales donde se informe y prevenga sobre el hurto informático, cómo evitarlo, poniendo en conocimiento la Ley 1273 de 2009, también cómo proteger los datos personales y qué papel cumple el Estado para garantizar la protección de la información.

Resumiendo lo planteado, el sujeto pasivo en el hurto informático puede ser una persona, natural o jurídica, y el delito de hurto puede cometerse por motivos económicos o por perjudicar los bienes patrimoniales de las personas o empresas, como se dijo desde un principio.

Así lo indica la doctrina penal, al establecer que el sujeto pasivo es quien goza de la titularidad del interés o bien jurídico tutelado, mencionado en el tipo penal, bien que sea amenazado o vulnerado por cometer una acción típica.

Por ejemplo, el caso más común en el delito informático, ocurre cuando se utiliza un cajero electrónico para retirar dinero: en el momento cuando el individuo hace el retiro de sus dinero, otro hombre ingresa (sujeto B) y le manifiesta a la persona que en su transacción hubo un mal procedimiento, le pide que introduzca nuevamente su tarjeta, no obstante, antes de realizar esa acción, el delincuente toma la tarjeta sin que la persona se dé cuenta y la inserta en el cajero, después le pide a la persona que digite su clave y cuando realiza esta acción, el sujeto B con un dispositivo manual clona la banda magnética de la tarjeta y como ha mirado la clave concluye su actividad.

Transcurrido un tiempo recibe notificaciones de alerta de los sistemas de seguridad del banco, que indican que se hicieron varias transacciones por una determinada cantidad de dinero; la víctima del hurto informático se dirige a la entidad y niega que haya hecho esas transacciones, por lo que presenta a la entidad bancaria su tarjeta original, y el banco le muestra el video de la cámara de seguridad dándole a conocer que el ciudadano recibe ayuda de un tercero que clona la tarjeta y registra la clave.

Como se evidencia el delito se comete en el momento en el que empiezan a sacar dinero del cajero automático y realizar transferencias de la cuenta del titular a un tercero ilegitimo, así se vulnera la seguridad bancaria.

Como afirma Grisales (2013), cualquier persona está en la capacidad de cometer la conducta punible, en este caso el delito de hurto informático al cual se hace mención. Según las denuncias interpuestas ante la fiscalía, se estableció que no es una sola persona quien comete el hurto por medio informático, sino que esta acción ilícita es realizada por varios sujetos que comparten la autoría y participan en los hechos punibles de diferentes formas.

Lo que aquí se evidencia es que las modalidades identificadas permiten establecer que, si se generan hurtos por medios informáticos y similares, es por la capacidad delictiva que cuentan los delincuentes para clonar las tarjetas de los usuarios de las entidades bancarias. Esto demuestra que los autores de este delito conexo al hurto informático suelen ser varias personas: uno de ellos instala o utiliza el dispositivo clonado y copia la información de la tarjeta en una banda magnética que se instalada en otra banda magnética, con el fin de obtener la contraseña de la tarjeta.

En ese orden de ideas, la persona que comete el delito de hurto informático puede ser una persona o un sujeto especializado en conocimientos informáticos, quien accede a un sistema

informático, telemático, o varias personas cometiendo clonaciones de tarjetas débito o crédito serán considerados como los cómplices, por lo que se convertirán en partícipes del delito.

De acuerdo con Grisales (2013), es por medio del hecho que se establecen las figuras expuestas desde lo penal, la primera es quien domina la acción de forma directa y ejecuta el verbo rector, la segunda es quien ejerce el dominio voluntario de un tercero para actuar como autor mediato, y el coautor quien ejerce el dominio funcional del hecho y participe.

Lo que significa que las personas que cometen un delito, que en este caso es el hurto informático, deben planear el delito y llegar a un acuerdo con anterioridad, para ejecutar el hecho punible, aportar conocimientos en materia criminal, por medio de su acción individual o colectiva, siendo necesaria para cometer el ilícito, por lo que el resultado obtenido sea delictivo y este tenga cierto grado de igualdad en el control de dominio.

De acuerdo con la explicación anterior, es autor directo quien realiza el verbo rector (el que hurte); por lo tanto, es quien domina la acción típica. En el caso de hurto informático, la persona que se dirige al cajero con la tarjeta clonada sustrae el dinero de la cuenta del titular o realiza la trasferencia a una cuenta bancaria de un tercer sujeto con quien ya existe un acuerdo para el depósito de ese dinero.

Aquí es donde surge el dominio subjetivo, se refiere al dolo de realizar la acción y negativo ya que su aporte es vital en la ejecución, pues la participación se da cuando se instala el dispositivo que clona, se retira y se copian los datos en nueva banda de tarjeta, por ello el aporte se necesita, aunque no tenga parte en la ejecución lo que hace que exista complicidad.

También se constata de acuerdo con Garces et.al (2020), que el sujeto en calidad de tercero tenía datos sobre la participación del delito, pues conocía la ejecución y como de iba a llevar a

cabo el plan, por ello, este individuo realiza un aporte fundamental al prestar su cuenta, debido a que permitió que se transfiriera el dinero del titular para su beneficio, lo que se calificaría como coautoría, debido a que tiene una participación funcional en el delito.

El hurto informático es un delito en el cual no participa un solo sujeto, ya que pueden ser varias personas bajo un común acuerdo, por lo que también se podría determinar que entra el acto de concierto para delinquir, como se establece en la Ley 1273 de 2009, en una conducta de hurto por medio telemático o similar, para perjudicar una persona que es la víctima a quien le cometen el hurto informático.

Además, el delito de hurto informático este asociado a la delincuencia organizada trasnacional, ya que la conducta punible de hurto informático tiene la capacidad por quien la comete de traspasar fronteras de diferentes países, pues se puede afirmar que la delincuencia transnacional está estructurada de acuerdo con Torres (2013), como el grupo de tres o más personas que durante algún tiempo se dedique a cometer delitos graves o tipificados con la intención de obtener algún beneficio de orden material.

Existen elementos de tipo objetivo y subjetivo, y son el sujeto activo y pasivo, así como lo es la conducta de hurto por medios informáticos y similares, al utilizar cualquiera de las modalidades previstas, que consiste principalmente en acceder o manipular las contraseñas de los usuarios, sin su consentimiento. Por ejemplo, acceder a los computadores para hurtar la información, comportamiento que pretende traspasar en términos informáticos las barreras de seguridad de los sistemas informáticos y soportes tecnológicos, que pueden ser contraseñas compuestas por códigos encriptados o suplantando la identidad del usuario.

A partir del 2009, con la interceptación ilegal de datos, empieza a ejecutarse en Colombia el delito de hurto informático. A partir de esa acción es necesario obtener la información y los datos del sujeto hombre o mujer, que son las personas a las cuales se les va a hurtar. Así, se interceptan u obtienen los datos con los que se ejecutará el accionar delictivo mediante una herramienta o un medio informático.

Para apropiarse ilícitamente de esa información, son utilizados programas que permiten la encriptación de códigos, método tecnológico que hace posible traspasar las barreras de seguridad de los sistemas informáticos y similares que contienen la información.

En Colombia, la Ley 1273 de 2009 regula y sanciona jurídicamente todas las conductas punibles que implican el acceso a los distintos medios informáticos y en relación con las TIC, ya que es posible cometer delitos desde una red de internet.

En relación con el desarrollo de las aplicaciones digitales y el avance mundial de la informática, la Sala de Casación Penal de la Corte Suprema de Justicia indica en la Sentencia SP-1245/15 que "en el delito informático existen principalmente dos elementos que son los bienes jurídicos tutelados que corresponden al patrimonio económico de forma inmediata y la información y datos de forma mediata" (CSJ Sala de Casación Penal, SP-1245/15, 2015).

El legislador señala que el presente tiene la suficiente capacidad, así sea ejecutado por medio informático o virtual, de transgredir la confianza y la seguridad de las personas en los distintos sistemas informáticos que pueden clasificarse como medios telemáticos, electrónicos o semejantes, aplicaciones digitales, etc.

La CSJ considera que es responsabilidad no solo de las entidades bancarias sino de las principales entidades que protegen el capital de los usuarios, que tienen la gran responsabilidad en

términos de seguridad, de suministrar *hardware* y *software* efectivos, con el fin de que se salvaguarde tanto el capital de los usuarios, como la información de las personas.

Asimismo, la CSJ señala que debe existir el beneficio de rebaja por reparación integral en relación con la persona que actuó en contra de la víctima, principio que contempla el Código Penal en Colombia, en el artículo 269, que expresa la rebaja de la mitad de la pena.

En la Sentencia SP-1245/15 (2015), se menciona además que si las personas que administran los establecimientos comerciales o los gerentes de las entidades bancarias son partícipes o cómplices, incurren en el delito de hurto informático, ya que esas personas tienen acceso a la información de las tarjetas de los usuarios.

Entonces, es preciso señalar que en términos de la teoría del delito, en la conducta punible de delito informático "el derecho penal califica para reprimir o castigar el delito y es por medio de la ley o el ordenamiento jurídico, que tipifica la conducta criminal que afecta a la sociedad" (Almanza, 2010, p. 91).

Por ende, el delito de hurto informático también presenta un nexo causal con conductas criminales, pues existe una voluntad del sujeto, que es lo que hace que la persona quiera hurtar por medio informático. La Ley 1273 de 2009 resalta que la persona que hurte por un medio tecnológico o similar también atenta contra el orden jurídico y la sana convivencia, pero que además la persona que hurta también se perfila como un sujeto de alta peligrosidad. Así lo explica un reporte del Centro Cibernético de la Policía Nacional:

En el que de acuerdo con Garces et.al (2020), se establece que cometer estos delitos y aquellos relacionados con la tecnología aumentaron en un 28% durante el 2017 en relación con el año 2016, esta entidad recibió 11.618 denuncias por la violación de delitos que se promulgaron en

la ley 1273 de 2009, entre ellos se encuentra el hurto por canales informáticos y similares, el cual recibió 6963 denuncias durante el 2017, y el delito por violación de datos personales 5117 casos.

El hurto informático en el país desde la ley 1273 se tífica por medio de manifestaciones fenomenológicas que se asocian con los delitos informáticos, frecuentemente estos son tratados como hipótesis jurídicas equivalentes a: 1) criminalidad informática en sentido amplio y 2) cibercriminalidad, términos que por supuesto tienen similitudes y semejanzas

El primero se refiere a las conductas tradicionales que se realizan por parte de un individuo activo, por medio del uso de sistemas informáticos con la consecuente lesión o peligro de los bienes jurídicos individuales o supraindividuales.

El segundo término, conocido como cibercriminalidad, se presenta con una serie de tipologías especiales que no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos, y se ejecutan a través de procedimientos informáticos que se caracterizan por cierta habilidad técnica, por lo que se puede caracterizar la gravedad de estos.

Tal como lo plantea Garcés et.al (2020), estas son las conductas típicas, culpables, antijurídicas que se dan cuando se utiliza un sistema informático que afecta los datos de los usuarios, así como sus intereses jurídicos que están titulados por el derecho como su patrimonio y derecho a la intimidad.

En consecuencia, el hurto informático implica una conducta con la cual se apoderan de la cosa o mueble ajena, a través de la manipulación de un sistema o medio informático, y de cierta manera al traspasar y burlar las medidas de seguridad informática.

Esta modalidad de hurto, en términos penales se materializa cuando el individuo o sujeto activo ingresa de manera ilegal o sin consentimiento de la persona, que se convierte en el sujeto

pasivo víctima de hurto informático; además, cuando se accede al procesamiento electrónico de datos, para entrar a hurtar la información o los bienes intangibles que necesite el delincuente informático. Por ejemplo, cuando se hurta un dinero de un cajero electrónico o se alteran los números de una tarjeta débito o crédito, y no es suficiente solo con esta acción, sino que además el individuo ingresa al cajero electrónico e instala bandas magnéticas para poder descifrar la clave de la cuenta bancaria de la víctima.

7.2.1 El sujeto activo en el delito de hurto informático

El sujeto es la persona o el individuo que en el contexto del delito informático posee las habilidades o características que no tienen los delincuentes comunes, pues tiene la capacidad para manejar los sistemas informáticos y semejantes a ellos. Su actividad delictiva la desempeña en lugares estratégicos, para no ser descubierto fácilmente. Se puede constatar que el sujeto activo en el contexto de delitos informáticos presenta unas características singulares.

Para las personas que hacen parte del aparato judicial, el delito de hurto informático ha sido una tarea compleja, ya que, como señala Garcés et al. (2020), es un arduo compromiso para los operadores judiciales identificar o acusar a una persona de ser un delincuente cibernético o informático, pues existen casos en los cuales no es suficiente la sustentación de la argumentación jurídica, al momento de poner en juicio a un delincuente que comete el delito de hurto informático, debido a que estos sujetos aceptan los cargos que se les imputan para acceder al beneficio de casa por cárcel, ya que precisamente este es un delito excarcelable y no siempre requiere de la pena intramural, por razones relacionadas con la sobrepoblación carcelaria o porque la persona que comete este delito, se acoge el beneficio de no tener antecedentes penales o cooperar con la justicia.

Otra falencia que existe es que se ha determinado en el artículo 269 i del código penal que el sujeto activo no está definido de forma específica en la norma, por lo que su naturaleza es indeterminada o no se ha identificado con claridad, debido a que el contenido normativo por hurto informático hace énfasis en el mecanismo de desapoderamiento de la cosa mueble ajena y no en la persona.

Así, el sujeto activo se vuelve indeterminado, y como lo argumenta la Ley 1273 de 2009, el que acceda a un sistema informático puede ser cualquier persona, no específicamente un ciberdelincuente. Además, el hurto informático no es cometido por una sola persona ya que también lo puede ejecutar un grupo de individuos que pueden ser denominados sujetos activos, por lo que surge la situación de coautoría.

7.2.2 El sujeto pasivo en el delito de hurto informático

En el delito informático el sujeto pasivo es la persona o el individuo que tiene la titularidad del bien jurídico que, por supuesto, la ley o quien la legisla tiene la obligación de proteger, sean personas naturales o jurídicas, ya que el delito de hurto informático al ser ejecutado por el delincuente cibernético no tiene ningún tipo de consideración.

La Ley 1273 de 2009 no señala en sí al sujeto pasivo de la conducta punible, lo que quiere decir que la norma es de carácter interpretativo. Lo que sí indica, es que el sujeto pasivo es quien en términos jurídicos es titular del patrimonio vulnerado y del dinero sustraído de manera ilegal.

Se sustenta entonces que el hurto por medios informáticos y semejantes desde el punto de vista tecnológico, de acuerdo con Garcés et.al (2020), se da cuenta se altera un sistema sin autorización o autenticación y la victima es el usuario al que corresponde la defensa.

Es decir, que para hurtar por medio informático es necesario y obligatorio adulterar un *software* o sistema informático accediendo a las contraseñas de las personas, sin que estas se den cuenta, obteniendo de forma ilegal la clave de acceso. Esto se logra instalando en los computadores o dispositivos móviles, por ejemplo, las aplicaciones digitales de las entidades bancarias en los teléfonos o computadores de los usuarios.

El hurto informático está descrito así en el código penal, como aquel que superando las medidas de seguridad informática, cometa conductas señaladas en el artículo 239, en el que manipule un sistema informático o una red telemática u otro sistema electrónico en el que suplante a usuarios ante los sistemas autenticados y autorizados que se encuentran establecidos, lo que incurrirá en penas tipificadas mediante el artículo 240 del código penal.

El hurto por medios informáticos en Colombia no afecta solamente el bien jurídico tutelado de la información y de los datos, sino que además transgrede los derechos a la intimidad, a la honra y al buen nombre porque se afecta la persona que se ataca por el medio informático, ya que la integridad se caracteriza por el libre desarrollo de la personalidad, la libertad de pensamiento, la condición social, la condición sexual, étnica, cultural o religiosa, principios del Estado social y de derecho.

El hurto informático está relacionado al acceso por medio telemático o similar. Acceder significa ingresar o entrar virtualmente a un determinado sitio de la red de internet, lo que implica la debida autorización de la persona que tiene a cargo el sistema de origen virtual; es decir, que ese ingreso implica conocer de recursos informáticos como contraseñas y programas que faciliten el ingreso a un sistema.

Ahora bien, este concepto del control de acceso se puede clasificar en tres principales pasos: el primer paso es la identificación, o sea, todo tipo de datos relacionados con la persona; el segundo es el soporte legal del sistema telemático o informático al cual se accede, y el tercer y último paso es investigar qué información se quería obtener, mediante un medio probatorio que se denomina el peritaje informático.

El peritaje informático se convierte en el medio probatorio que demuestra ante una autoridad competente. En el caso colombiano ante un juez penal que está facultado con esa competencia. El peritaje permite descifrar o descubrir cómo ingresaron al sistema por medio de una evidencia digital, como la dirección IP, que facilita la identificación de protocolo del internet y hace posible la comunicación a través de esta red, con un número de protocolo específico para cada usuario en línea, ya sea en el envío de correos electrónicos, la transmisión de video o la conectividad a un sitio web.

Como lo refiere Paloma (2012), la comisión del delito de hurto informático se da por medio de un sistema de navegación en la red, por ello, el hacker se vale de sus conocimientos para maniobrar sin la autorización de los titulares de las cuentas bancarias y de esta forma extrae el dinero de depósitos. Esta modalidad se identifica en el país cuando se usan "dispositivos electrónicos de manera clandestina, porque no existe una norma que controle o regule la obtención de estos dispositivos cuando son requeridos por las personas que residen en el territorio nacional" (Palomá, 2012, p. 153).

Como se ha venido diciendo, el delito informático es toda clase de conductas punibles que se desarrollan a través de un portal web. Es el caso de cuando un *hacker* con amplios conocimientos en informática o quien tenga acceso a internet, hurta lo que es conveniente para él o en beneficio de un tercero. El hecho más recurrente en Colombia es cuando se comete el hurto en una cuenta

bancaria, sin que la víctima sospeche de la transferencia, una acción con altas pérdidas económicas y de infraestructura tecnológica en el país.

Dicho de otro modo, el hurto informático es toda violación jurídica que ocurre virtualmente en el ciberespacio, y va mucho más allá que una simple conducta delictiva, pues desde el contexto colombiano transgrede la seguridad nacional y quebranta el principio del Estado social de derecho, pues ese delito tiene alcances tan graves como las pérdidas económicas y muestra los pocos conocimientos que hay en seguridad informática en la sociedad nacional.

Es necesario recalcar que el medio informático es todo elemento telemático, digital y de acceso a la plataforma en línea de un sistema informático para desarrollar determinada tarea en los computadores, que se puede clasificar en páginas web, correos electrónicos, programas de aplicación, discos duros portables, memorias USB y dispositivos de extracción.

En otras palabras, el medio informático es el objeto sobre el cual cae la acción del hurto informático, entonces se convierte en el instrumento que se utiliza para ejecutar toda actividad que implique el uso de un computador. Puede entenderse como la herramienta que se usa con fines educativos, tecnológicos y de explotación de conocimiento para darle un uso óptimo. De acuerdo con la afirmación anterior, corresponde a la seguridad informática de las entidades estatales y privadas que hay en el país, combatir y contrarrestar el delito informático.

El uso de las redes sociales y demás plataformas tecnológicas ha facilitado y fortalecido la capacidad de acceder a internet, pero ha aumentado la capacidad de la delincuencia para delinquir y hacer daño a través del medio informático, pues en Colombia y en el mundo, la tecnología ha desarrollado diversas aplicaciones digitales.

Es necesario que se entienda que el medio informático se crea y se pone en funcionamiento con varios fines: educativos, culturales, económicos, sociológicos y para infraestructura tecnológica, pero también se asocia con una conducta antijurídica y tipificada que es el delito de hurto informático, de tal manera que la seguridad informática que debe aplicarse al medio informático tiene similitudes al gran avance tecnológico que ha ocurrido en los últimos años. Entonces, la educación fomenta el pensamiento inteligente en la formación íntegra de la persona.

Asimismo, como lo establece Vélez (2022) el individuo se forma para tener buenos principios y conductas a través de los medios existentes, en este caso para emplear medios informáticos, por ello, la educación debe responder a las necesidades que tengan las personas en la era tecnológica, esta gestión para aprender debe contribuir al desarrollo de las capacidades, lo que ayuda al desarrollo de la sociedad.

De esta forma, la ejecución de un delito informático se puede dar por un estudiante o individuo que acceda al sistema informático, lo que lo diferencia del *hacker* o ciberdelincuente es que este individuo posee amplios conocimientos en informática y sus ramas anexas, lo cual le permite hurtar en el sistema informático sin ser identificado con facilidad. También debe señalarse que los ciberdelincuentes poseen programas, aplicaciones y métodos que son efectivos para evitar ser rastreados en la web y de este modo no ser judicializados o puestos en juicio por las autoridades competentes.

Con el transcurso del tiempo y en el contexto de la pandemia con la aparición del covid-19, al inicio del 2020 la tecnología se convirtió en una necesidad, desde el aspecto laboral y personal, porque la forma de trabajar dio un giro de 180 grados, ya que pasó de ser algo presencial a convertirse en un aspecto virtual, lo que abrió la posibilidad de que el acceso a la información se

diera mucho más rápido que antes y permitió que las personas accedieran a la búsqueda de su información corporativa desde un dispositivo o plataforma tecnológica con acceso a internet.

Al mismo tiempo facilitó que surgiera la modalidad delictiva del delito de hurto informático. Según estadísticas del Ministerio de Tecnologías de la Información y las Comunicaciones, durante el primer trimestre del 2022 se presentaron 6.407 casos de acceso abusivo a sistemas informáticos con fines de hurtar la información; se evidencia que hubo un total de 11.078 casos de hurto informático, lo cual indica que hubo un aumento de un 15 %.

Para Rivera (2020), el hurto por medios informáticos busca obtener un grado de dominio en el patrimonio no solo económico, sino todo el que le represente beneficio alguno de la víctima a la cual se va hurtar, que en ese caso es causar una pérdida del patrimonio económico, hecho que se lleva a cabo por medio de la clonación de una tarjeta de crédito, obteniendo la clave de esta; pero si en el momento en el que el delincuente va a sustraer el dinero y la víctima no cuenta con el saldo o el cajero presenta fallas en su funcionamiento tecnológico, se puede decir que se pretendía hurtar el dinero.

El hurto informático busca desestabilizar el ordenamiento jurídico social porque es un delito que genera un grado de desconfianza en la sociedad, ya que intimida no solo a las personas que residen en Colombia, pueden ser connacionales o extranjeros, sino que pone en alerta a las autoridades para que se investigue desde el delito la conducta de un ciberdelincuente. Esta conducta ataca la seguridad de cualquier entidad no solo bancaria y permite evidenciar que la delincuencia tiene conocimientos y gran capacidad para hurtar por medio de un dispositivo informático.

La Corte Suprema de Justicia sustenta, por medio de la Sentencia SP-1245/15, que en el hurto informático también existe la conducta, pues en la doctrina penal se establece que desde el hurto informático el legislador pretende demostrar la existencia del otro tipo penal denominado la lesión porque es parte del interés tutelado, como el patrimonio económico y la seguridad, desde la perspectiva del tráfico de información y los sistemas informáticos o telemáticos. También lo es de la obtención del resultado, debido que para la consumación del hecho debe desaparecer el dinero siendo ese el perjuicio, en términos económicos, para quien tenga la posesión de la cosa.

Al inicio de la pandemia en Colombia, el 6 de marzo del 2020, se dio el giro para la apertura al uso tecnológico e informático en la vida laboral de las personas. El cambio fue positivo porque inició la implementación de las TIC y lo concerniente a la virtualidad, y se declaró el internet como un servicio público esencial mediante la Ley 2108 del 29 de julio de 2021.

Pero, así como hubo cambios positivos, existen ahora nuevas formas de hurtar por medio informático y de vulnerar, a través de este delito, la información de los usuarios, entendiendo esta como los datos concretos compuestos por elementos, clasificados en imágenes, escritos, nombres y apellidos de las personas, que se clasifican según su país de origen, fecha de nacimiento y edad, como también información crediticia, bancaria e historial médico.

En tiempos de pandemia las TIC pasaron a convertirse en herramientas necesarias en la vida de cada persona, desde tres conceptos: la informática, la electrónica y las comunicaciones, con el fin de generar una interacción e interactividad virtual de los usuarios mediante una red.

Debido a las restricciones de movilidad interpuestas por el Gobierno, los colombianos y extranjeros residentes en el país pasaron de la modalidad de trabajo presencial a la modalidad virtual, lo que permitió que el manejo de datos fuera más riguroso y se adoptaron medidas en las

entidades financieras. Muchos bancos se vieron en la necesidad de brindar atención en línea y por chat virtual, con el objetivo de intercambiar y rectificar la información del usuario para realizar cualquier transacción financiera, según los servicios ofrecidos por el banco, con la autorización del usuario.

Para Sánchez (2022), las políticas de gobierno en Colombia en los años recientes permitieron un cambio en la forma de vida de las personas, en relación con el manejo de la información que está conformada por datos. Con el fenómeno de la pandemia los ciudadanos tuvieron que afianzarse en el uso de plataformas tecnológicas y demás herramientas digitales que están en la web, las cuales se utilizaron para estudiar, trabajar y adecuar todo tipo de información ya contenida en bases de bancos digitales.

Fue un cambio estructural que produjo la creación de programas digitales para el acceso a servicios en línea, interacción en redes sociales y acceso a aplicaciones digitales, tanto de entretenimiento como de uso personal. Por esta razón, el manejo de datos en Colombia cambió drásticamente, pues se vio reflejado en el ordenamiento jurídico y modificó las normatividades que protegen los datos personales.

A medida de que las personas cambiaban su estilo de vida y las formas en las que se relacionaban, compartían su información, la delincuencia evolucionaba para crear nuevas maneras de delinquir, tales como reestructurar, identificar y obtener la información personal de las empresas y de las personas, por ello, era prioritario que en el país se cumpliera de forma estricta la normativa para salvaguardar el derecho a la información, tal como lo refiere la sentencia C-748/11 el 2011, en la que se establece que los datos personales deben estar blindados con garantías constitucionales que se expresan en la constitución mediante los artículos 15 y 20, en los que se establece que las personas cuentan con el derecho de rectificar y actualizar la información que hayan estipulado en

los bancos de datos del país mediante la ley de habeas data para salvaguardar los datos personales en Colombia.

La protección de datos se rige por medio de la Ley 1581 de 2012, que se encarga de regular la protección de datos personales, es decir, protege también la información de entidades públicas y privadas, y el delito de hurto informático puede afectar a todos los anteriores.

7.3 ¿Cómo se afecta la información de los datos personales de los usuarios por medio del delito de hurto informático?

La afectación de la información de los datos personales se presenta cuando se accede indebidamente a la información de bancos de datos y se consuma cuando el autor, es decir el sujeto que comete la acción, logra sacar del círculo de dominio la cosa que se hurta (el dinero) mediante el uso de un medio informático o elemento telemático, en beneficio propio o de un tercero.

La Organización de Estados Americanos (OEA) establece la seguridad y el orden para instaurar una sana convivencia, y partiendo del argumento que la protección de los datos corresponde a cada país en relación con su constitución, en el caso de Colombia se entiende que los datos de los usuarios son privados y que es obligación del Estado salvaguardarlos para garantizar su protección.

En Colombia solo es posible acceder a la información de los datos de una persona con autorización expresa, salvo cuando la ley lo requiera; por ejemplo, en nuestro país se entiende que la cédula de ciudadanía es el único documento válido para la identificación de un ciudadano.

Así se desarrolla el derecho del *habeas data*, y se determina un ámbito de aplicación en Colombia. De esta manera, las entidades bancarias deben cumplir el secreto bancario, que es una

protección que se rige desde el principio constitucional en el que se obliga y se les permite a las entidades financieras guardar los datos relacionados con sus clientes o sus productos.

Al momento que se acceda a estos datos ilegalmente, se hurta la información; para evitar que se consuma en delito de hurto, el Estado colombiano firma el convenio sobre la ciberdelincuencia, o de Budapest, el cual evidencia que el fraude informático es un delito que se relaciona con el hurto informático y la violación de datos personales, pues la legislación europea se enfoca en este tipo penal y los legisladores determinan que los delitos de hurto e interceptación ilícita de datos personales surgen a partir del fraude informático. Este tratado que Colombia adopta es el primer hecho que posibilita la creación de la Ley 1273 de 2009, que especifica el delito de hurto informático.

Para que se consuma el delito informático de hurto por medio telemático o similar es necesario obtener de manera ilegal los datos de la víctima que se va a perfilar o a seleccionar. Según la Sentencia C-094/20 que se emitió por la Corte Constitucional (2020), el derecho a la intimidad se encuentra reconocido en el artículo 15 de la Constitución Política de 1991, y manifiesta que todos los ciudadanos, connacionales y extranjeros, que residan en Colombia cuentan con su derecho a la intimidad personal y familiar así como a su nombre, y el Estado debe hacerlos respetar; teniendo en cuenta toda correspondencia que involucra las formas o los medios de comunicación privada que son inquebrantables y solo pueden ser interceptadas o rastreadas bajo orden expresa judicial, en los casos y con las formalidades que establezca la normatividad jurídica, el estado puede exigir la presentación de la contabilidad en los términos en los que lo señale.

El hurto informático lesiona al individuo porque ataca la privacidad que existe en la información que solo le compete a la persona que desea, información que está contenida en los distintos bancos de datos, y puede estar clasificada en información crediticia, académica, laboral

o científica, que quieren hurtar las personas que tienen acceso a un sistema informático; es decir, un ciberdelincuente que cuente con conocimientos en el área de la informática y conexas a esta disciplina.

Se debe aclarar que el delito de hurto informático se diferencia en el contexto del continente europeo al continente suramericano: los europeos consideran que las conductas punibles como el delito de hurto informático son actos ilegales que se cometen utilizando una herramienta que es un computador o medio telemático, y crearon normatividades como fundamento jurídico basándose en la ciberdelincuencia, que es toda estructura delictiva que delinque en línea o a través de un sistema virtual, lo que quiere decir que un delincuente que comete un robo a mano armada en determinando lugar, tiene la misma capacidad delictiva para realizar un hurto por medio de un sistema informático.

En ese sentido, se considera que la tecnología ha evolucionado a gran velocidad y ha sido el puente para accionar una modalidad delictiva que se conoce como los ciberdelitos o delitos informáticos; en este caso, el hurto informático ataca el ciberespacio o la red informática de cada nación y a los ciudadanos, al acceder a sus datos o información sin la debida autorización.

Se debe aclarar que el delito de hurto informático tiene diferencias en términos jurídicos, en Europa y en Latinoamérica, la primera diferencia es que para los europeos los delitos informáticos en especial el delito de hurto informático corresponde a conductas ilegales, que se cometen empleando o utilizando una herramienta informática o medio telemático, partiendo de ese argumento, ellos crean el concepto de la ciberdelincuencia, como toda estructura delictiva, que delinque en internet o a través de un sistema virtual.

Es así que países como España han adoptado una normatividad que regulen las conductas punibles desde el uso de medios informáticos, se evidencia que los españoles establecen un movimiento legislativo que busca tipificar todo lo relacionado con los ciberdelitos o delitos en línea, en especial el hurto informático, una de esas normas fue establecida en el convenio de Budapest para regular los delitos informáticos, tratado que se firmó el primero de julio de 2004, ya que, en los años de 1992 y 2000 se dio un gran aumento respecto al uso de ordenadores y de igual forma de comportamientos que vulneraban personas, esto sobrepasando a los estados europeos, por la falta de normas en el uso de sistemas informáticos y tecnologías de la información.

7.4 El hurto informático en Colombia a partir de la Ley 1273 de 2009

En materia penal, el hurto informático está establecido en Colombia por medio de la Ley 1273 de 2009, que se denomina la ley de delitos informáticos, que en esencia tiene como objetivo proteger el bien jurídico tutelado, en cuanto a *la protección de la información y de los datos*, siendo uno de los mayores logros no solo en legislación penal, sino que además incorporó el concepto de medios informáticos o relacionados a estos.

Sin duda alguna, el hurto informático en Colombia, a partir de la mencionada ley, se fundamenta en el acceso a las TIC, en relación con el desarrollo de las aplicaciones digitales y el avance mundial de la informática. Con respecto a lo anterior, la Corte Suprema de Justicia, según lo indica la Sentencia SP-1245/15, manifiesta que "en el delito informático existen principalmente dos elementos que son los bienes jurídicos tutelados que corresponden al patrimonio económico de forma inmediata y la información y datos de forma mediata" (CSJ Sala de Casación Penal, SP-1245/15, 2015).

La Sentencia SP-1245/15, 2015 señala además como posibles personas partícipes o cómplices, que en el delito de hurto informático son identificadas como las personas que administran los establecimientos comerciales o los gerentes de las entidades bancarias, ya que esas personas tienen acceso a la información de las tarjetas de los usuarios. De ser identificadas como cómplices también tendrían que pagar por estos delitos.

Para Almanza (2010), en términos de la teoría del delito, el derecho penal está calificado para castigar el delito por medio de la ley y el ordenamiento jurídico de cada Estado, a partir de la potestad del Estado, para sancionar la conducta criminal que afecta a la sociedad desde la tipificación del delito y todas aquellas contravenciones en las cuales está involucrada la nación. En el caso del hurto informático, los datos personales de los colombianos y las personas que residen en el territorio nacional recaen sobre el Gobierno nacional como jefe máximo de Estado (*ius puniendi*).

En este caso, el derecho penal desde la ley de delitos informáticos (Ley 1273 de 2009), persigue y sanciona dichos delitos, creando un bien jurídico tutelado, que se conoce como *de la protección de la información y de los datos*, en relación con el debido uso y la preservación de las TIC y todo lo relacionado con las comunicaciones, lo que quiere decir que el Estado es el primer responsable de garantizar la seguridad y el bienestar de la ciudadanía, desde la protección de la información y el manejo que a esta se le dé desde los bancos de datos, para que no se hurten por medio informático y no se exponga la integridad de las personas. En eso tienen un papel importante los jueces penales de Colombia y tribunales, según corresponda.

Por ende, el delito de hurto informático presenta un nexo causal con conductas criminales, pues existe una voluntad del sujeto que es lo que hace que la persona quiera hurtar por este medio. Por ello, la Ley 1273 de 2009 resalta que la persona que hurte por un medio tecnológico o similar

también atenta contra el orden jurídico y la sana convivencia, pero que además la persona que hurta también se perfila como un sujeto de alta peligrosidad.

Según Garcés et al. (2020), se puede definir como hurto informático el mal uso de la información y de algún medio informático que se emplea para el manejo desde el aspecto tecnológico, todo método que cause un perjuicio en la libertad de las personas o que ponga en riesgo su patrimonio o propiedad, no solo privada sino intelectual; por ejemplo, divulgar conocimientos relacionados con la empresa para la cual trabaja, o aspectos académicos que ponga en riesgo alguna entidad universitaria, o información de su sistema de seguridad social, pues el hurto informático se hace con ese fin de tener conocimiento sobre los datos de una persona para obtener un beneficio propio.

Como ya se ha mencionado, el hurto informático en Colombia se persigue y es castigado a partir de la Ley 1273 de 2009, así las cosas, el hurto informático se define como una conducta con la cual se lleva a cabo el apoderamiento de lo ajeno por medio informático, por medio de la manipulación de un sistema o medio informático, y de cierta manera al transferir y burlar las medidas de seguridad informática es que se comete el delito.

8. Los delitos informáticos desde el marco legislativo internacional, la Ley 1273 de 2009 y otras legislaciones

8.1 El convenio de Budapest

El Convenio de Budapest o tratado sobre delitos cibernéticos es el primero a nivel internacional que busca combatir los delitos en Internet a través de la conjunción de leyes entre algunos países interesados en combatir el cibercrimen, mejorar las técnicas de investigación y aumentar la cooperación entre los países que firmaron. Este se elaboró en el Consejo de Europa en Estrasburgo y participaron de manera activa Canadá, Japón y China.

El convenio mencionado hace referencia, en el Título 2, artículos 7, 8, y 9, a los siguientes delitos informáticos: fraude informático, falsificación informática, y delitos que se relacionan con la pornografía infantil; este último delito no será tenido en cuenta en el presente trabajo.

El Estado colombiano adopta el convenio de Budapest, para proteger desde la legislación internacional la información y los datos de los usuarios. Cada nación, de acuerdo con sus principios, debe mantener su seguridad y estar alerta contra la nueva era del terrorismo cibernético que busca ejecutar ataques por medios informáticos, que pueden ser hurto de bases de datos, información personal y confidencial, entre otros.

Por medio de este convenio se aplica el principio de solidaridad universal, que tiene como objetivo hacer efectivo el bienestar común de la sociedad, al hacer referencia al Estado social de derecho, relacionado con la función jurídica que tiene el país desde la potestad punitiva del Estado para hacer frente al delito. Cabe destacar que Colombia, por medio de los magistrados de la Corte Suprema de Justicia, firmó el Convenio de Budapest (Hungría) contra la ciberdelincuencia, que se

menciona en la Sentencia C-224 de 2009 emitida por la Corte Constitucional (CC) en el que existe un argumento jurídico de que la ley debe confrontar y castigar la ciberdelincuencia o quien comete el delito de hurto informático, pero se requiere una ayuda en términos de cooperación internacional, en lo que concierne en materia penal estructurada, rápida y eficaz contra el delito de hurto informático y demás delitos conexos.

Debido a que este convenio es necesario para la prevención de actos que van en contra de la confidencialidad y la integridad de los sistemas informáticos; así mismo el abuso de las diferentes plataformas tecnológicas, redes, datos y sistemas, a través de la tipificación de esos delitos, como lo manifiesta este tratado, así como los poderes de cada país, entre ellos Colombia, para contrarrestar y combatir de forma eficaz y segura estos delitos. Al momento de detectar estos delitos se investigan y sancionan, tanto a nivel nacional como internacional, para crear alianzas que permitan una cooperación internacional expedita y confiable (CC, C-224/19, 2019, pp. 6-7)

El convenio de Budapest entro en vigor en el primero de julio de 2004, y fue ratificado por 47 países, entre ellos Colombia. Este convenio se convirtió en el puente para la creación de la Ley 1273 de 2009 o ley de delitos informáticos.

8.2 Ley 1273 de 2009 o ley de delitos informáticos y otras legislaciones

El ordenamiento jurídico de la Ley 1273 de 2009 ha contribuido al enfrentamiento de delitos informáticos, esta ley incluye procedimientos y políticas para garantizar la seguridad de la información, también define las acciones penales de las personas que incurren en deliticos establecidos por la norma.

La norma nace gracias a la aprobación del convenio de Budapest, un antecedente jurídico que se desarrolló a partir de la ley 1928 de 2018, para que Colombia entrara a formar parte de los países que adoptaron el tratado en materia de infraestructura tecnológica y de redes de internet, con el objetivo de contrarrestar los delitos cibernéticos, como es el hurto o fraude informático, debido a que en el país no existe la suficiente formación en términos pedagógicos y académicos para fortalecer la protección de datos y seguridad informática que se pone en uso las diferentes redes y plataformas tecnológicas que hay en la red.

Aunque gran parte de la población colombiana no tiene acceso a un computador ni a internet, que posibilite la entrada a la era digital, poco a poco se va superando la brecha digital en el país. Los usuarios deben estar informados sobre los peligros que hay al acceder a las redes y sobre la seguridad informática.

En relación con lo anterior, principalmente la ley 1928 de 2018 garantiza el derecho que tienen los colombianos y extranjeros que residen dentro del territorio nacional para que en términos jurídicos se realice la debida protección de la información, pero el estandarte que compone la norma de la cual se habla es la tipificación de los delitos que destruyan, obstaculicen, borren los sistemas informáticos de los usuarios o redes de infraestructura informática.

El objeto de la norma es establecer que es un sistema informático, definido como todo dispositivo o conjunto de estos que se interconectan o relacionan entre sí y permiten la ejecución de un sistema o programa. Asimismo, establecer el significado del dato informático cualquier contenido de información o conceptos de una forma de procesamiento físico o digital, incluido en un programa que se diseña con la finalidad de que un sistema informático ejecute una tarea o función específica.

Pues estos sistemas proporcionan y proveen servicios no solo de comunicaciones sino también de procesamiento de información para fines, médicos, comerciales, financieros, comunicaciones (redes de telefonía), servicios postales entre otros.

Además, la Ley 1228 de 2018 adopta una serie de medidas para la aplicación de la norma a nivel nacional, una de estas es la delimitación que se hace para la interpretación de la norma con relación a los delitos que van en contra de la confidencialidad en términos de información, a la integridad que debe existir en el tratamiento de datos, así como la disponibilidad de estos, y por último el suministro de sistemas informáticos.

Estos delitos de los cuales hace mención la ley son el acceso ilícito o de manera indebida, la interceptación ilegal, la interferencia u obtención ilícita de datos, interferencias en el sistema o abuso de los dispositivos.

Por esta razón, el hurto informático en Colombia da a conocer la falta de conocimiento en cuanto al objeto de la Ley 1273 de 2009, pues desde un principio se llegó a pensar que los elementos que se hurtan por medio de la modalidad que se expone en este trabajo, no son punibles. Esta ley establece qué son los delitos informáticos y cuáles son los castigos para quienes incurran en estos hechos.

Lo que se da a entender, es que al no considerarse que sea tangible la cosa que se hurta, no pueden ser visibles de forma física, en el entendido que en el hurto informático se puede dar el delito, pero a los bienes o el dinero que está representado de forma inmaterial, por ejemplo, las acciones de una sociedad, dinero que se traspasa de una cuenta bancaria a otra sin el consentimiento de los usuarios, por lo que los datos se convierten en el medio principal para cometer el hurto informático y calificado, que en ese caso también se puede dar.

El tipo penal que se aborda principalmente es el de hurto a través de algún medio informático, pues la ley mencionada presenta una ineficacia jurídica; cuando se redactó esta ley para ponerse en marcha, se va a proteger la información de los usuarios, por lo que el delito informático también emplea el uso de los neologismos en el campo científico de la informática, por ejemplo, la creación de números binarios.

Asimismo, este delito en Colombia se malinterpreta ya que el término informática solo se delimita al uso general de un computador, pero al pasar a los términos de cómo establecer el hurto informático, se describe como transferir de un activo determinado con la ayuda de habilidades en informática bastante avanzadas para causar un perjuicio a un tercero.

De acuerdo con lo antes mencionado, existe una diferencia entre el delito informático y el ciberdelito: el primero consiste en que se comete un hecho ilegal utilizando un medio como el computador y demás tipo de tecnología, como puede ser dispositivos como *smartphones* y tabletas digitales que se caracterizan por tener *hardware* o *software*, pero que sus sistemas operativos sean de marcas de tecnología como Android de Google o iOS de Apple.

En ese sentido de acuerdo con Gonzáles (2017), los ciberdelitos son diferentes de los informáticos, debido a que es en el ciberespacio donde se desarrollan y se consuman sin que existan de forma necesaria en el mundo material.

Por lo anterior, las entidades bancarias deben enviar un aviso o comprobante electrónico que haga constar como soporte legal que se hizo esa transferencia, pues el hurto informático involucra tanto a las entidades bancarias como a las personas que son víctimas de este delito, ya que afectan a los usuarios de los bancos, no solo penal, sino civilmente. Motivo por el cual, el dinero que sea designado en los bancos o en cualquiera de sus oficinas que se encuentre en los

distintos departamentos o municipios del país, tiene una seguridad especial y se informa por medio de un desprendible electrónico o telegrama digital u oficio en forma física del estado de cuenta, envíos y transacciones, tanto fuera de Colombia y de países del extranjero con la que los bancos tengan la alianza; ahí se determina el valor de las transacciones, la denominación de los billetes y los sistemas de acceso, como el cajero automático.

Una de las características que asegura el dinero o la trasferencia de activos, es el cambio periódico de las claves a los sistemas de información, pero en caso de retirar el dinero físico, el banco emite las órdenes bancarias con unos números designados por la entidad para evitar el delito de hurto a través de medios informáticos y así prevenir a los clientes de una posible estafa.

En consecuencia, la persona que comete el hurto informático, es decir el delincuente cibernético que se conoce como el *hacker*, posee unas características especiales; estas personas son descritas como individuos socialmente aislados, es decir, que tienen pocos amigos o no frecuenta lugares que sean concurridos socialmente. También se cree que poseen un coeficiente intelectual bastante alto, lo cual implica que los conocimientos que maneja no son iguales para las personas del común, y se destaca por tener altos gustos por la informática y la computación. Este es el perfil del delincuente cibernético.

Por otro lado, existe una sola diferencia entre el concepto de delitos electrónicos e informáticos. Un delito informático se comete para causar un perjuicio a un tercero, accediendo sin su autorización a un sistema informático, por ende, se debe proteger el bien jurídico tutelado de la información; el delito electrónico se encuentra tipificado, pero en este caso se interpreta desde la captación ilícita de datos, lo que se considera que es conexo a los delitos informáticos.

Además, el primer antecedente normativo está relacionado con el proyecto de Ley 042 y 123 de 2007, que se había tratado con anterioridad en el Congreso de la República, pero que por motivos de ámbito político tuvo falencias al momento de ser presentado y aprobado. Debido a estos hechos, se denominó el bien jurídico tutelado de la protección de la información y de los datos, argumento que es válido porque hace referencia a los tipos penales en los que se viola la disponibilidad de información y son de tipo punitivos.

En cuanto a este antecedente jurídico, que se constituye como hurto informático, se caracteriza por la instalación de un programa en el computador que facilite la divulgación de esos datos que atentan contra la integridad del sistema informático. Por ejemplo, se encuentran almacenados en un sistema informático que pertenezca a una entidad pública, como la Fiscalía y la Procuraduría, o a las entidades y demás compañías que hagan parte del sector financiero.

Asimismo, hay delito informático cuando existe una relación de carácter contractual de una persona que tiene una vinculación no solo laboral sino personal con el propietario de los datos, para que esa persona hubiera obtenido beneficio propio o beneficio para un tercero. También cuando se dan a conocer datos sin el conocimiento de los usuarios, en este caso los datos personales o auténticos de un sistema, argumentos que desde un principio fueron expuestos por el proyecto de Ley 042; esas conductas se tipifican como el espionaje informático.

La informática entra a conformarse como una rama de las matemáticas, gracias a la secuencia lógica que proporciona unos resultados numéricos que tienen la orden determinada de un *software* para enviar, recibir o captar una información compuesta por mensajes de datos de manera aleatoria, lo que hace posible desarrollar conocimiento y creatividad para ejecutar programas tecnológicos que desarrollen el descubrimiento y la ejecución de todo tipo de información.

Por ello, cuando se termina la segunda guerra mundial nacen los derechos humanos gracias a una declaración con antecedentes jurídicos y culturales que fue enunciada el 10 de diciembre de 1948. El artículo primero de ese documento especifica que todas las personas nacen con el principio de la equidad, es decir, libres e iguales a la ley y, por lo tanto, tienen el deber de razonar y comportarse bajo todos los preceptos de la ley.

Cada individuo está identificado como una persona única que lo diferencia de los demás: su lugar de nacimiento, el lugar de domicilio y el país que le va a otorgar la nacionalidad. De esta manera, surge el concepto de *habeas data* que está adherido a los derechos fundamentales. Este concepto significa tener los datos en tiempo, es decir, al momento, al instante; acción que se convierte en un derecho fundamental, por lo que cada persona, sea natural o jurídica, tiene derecho a solicitar información referente a sí misma, como la de obtener, rectificar o corregir información según las disposiciones de ley.

Por consiguiente, la ley de delitos informáticos (1273 de 2009) se encarga desde la doctrina penal de darle nacimiento al bien jurídico que se ha tutelado por la prestación de los datos, esto evidencia que tal como lo establece Ojeda-Perez (2011), la diversidad de sistemas de información con la que cuentan las organizaciones, sumado al cambio de las TIC han generado transformaciones en los mercados, las organizaciones y el mundo moderno.

Desde esa misma perspectiva, la tecnología es un campo muy amplio, lo que implica que los sistemas de información se vean obligados a actualizarse, es decir, la actualización de datos, de *software* o de aplicación que van a darle soporte para que puedan funcionar esos programas, prestando un servicio de óptima calidad con amplios cambios; eso involucra a todas organizaciones, sean empresas públicas o privadas, y sociedades de personas naturales o jurídicas.

Cuando la información es obtenida por medio del hurto, se entiende que primero se vulneró el bien jurídico de la información y que por tanto se quebranta el orden del Estado social y de derecho; y segundo, se comete un delito que se tipificó en el artículo 269i del Código Penal colombiano, el cual especifica que quien por medios informáticos o semejantes traspase los sistemas de seguridad, suplantando la identidad del usuario, de los sistemas que esa persona tenga a cargo, está incurriendo en delito.

Es frecuente que el hurto se cometa por medio de los sistemas de información de los bancos, se obtienen las contraseñas bancarias por falsas llamadas que realizan empleando el sistema de *contact center* haciéndose pasar por representantes de cualquier entidad bancaria o, en su defecto, como asesores del mismo banco, especialmente si son personas que cuentan con la información completa de los usuarios: nombres, apellidos, cédulas, lugares de trabajo y la información de sus números de tarjeta débito o crédito.

Respecto al hurto por medio de los sistemas de información, se considera que es un delito que va en aumento en el país. Al respecto, Granados & Parra (2016), establecen que debido al aumento de los delitos informáticos y transferir sin consentimiento la información, las personas padecen detrimentos en su patrimonio que les genera grandes pérdidas económicas y de sus datos, ya que los delincuentes acceden a esta información.

Hay que mencionar que el Estado debe estar en la capacidad de vigilar qué entidades son las que cumplen con el procesamiento de datos de la información, y quiénes son las personas que ocuparán cargos en las entidades estatales (los gerentes y los directores ejecutivos), ya que ellos serán los garantes del manejo de la información. Esto significa que estos deben conocer la ley que se refiere al bien jurídico de la información y el tratamiento de los datos.

Lo anterior implica que la nación debe contrarrestar estos delitos desde la potestad punitiva del Estado (*Ius puniendi*), es decir que a partir del Estado social de derecho, el ejercicio de poder y libertad según Merlano (2017), se establecen límites para regular las conductas del Estado, lo que garantiza una vida civilizada.

Lo que quiere decir que el Estado tiene que sancionar y castigar penalmente la conducta delictiva que se encuentra en el delito de hurto informático, existe la potestad para que constitucionalmente se proteja el bien jurídico tutelado que se denomina “de la protección de la información y de los datos”.

De igual forma, en el hurto informático está el objeto en el caso jurídico en el que recae la acción: en este delito es una cosa mueble ajena el dinero, ya que se puede palpar y tocar, lo que de acuerdo con Abushihab (2016), se trata de cosas físicas en las que es posible un apoderamiento material, por ello quedan excluidas las cosas inmateriales, se traslada esto a la manipulación de dinero documental, escritural o contable.

9. Resultados

El uso de los sistemas informáticos y las TIC es parte fundamental de la vida actual y son imprescindibles en los ámbitos empresarial, personal, de salud, de comunicación y de bienestar social, sin embargo, estos avances tecnológicos también traen consigo aspectos negativos como los denominados delitos informáticos que lesionan o causan daño a la sociedad y la economía, por lo cual requieren una protección integral del Estado.

Los delitos informáticos en Colombia se rigen en materia penal por medio de la Ley 1273 de 2009, conocida como ley de delitos informáticos, esta norma tiene como fin castigar jurídicamente a los ciberdelincuentes que acceden abusivamente a un sistema informático, al que obstaculice de manera ilegítima un sistema informático o redes de telecomunicaciones, el que intercepte datos informáticos u ocasione un daño informático, produciendo, traficando, adquiriendo, distribuyendo, vendiendo, enviando, introduciendo o extrayendo del país un *software* malicioso o programas de computación de efectos dañinos; el que incurra en la violación de datos personales, y el que incurra en la suplantación de sitios web para robar datos personales. Estos delitos se encuentran descritos y tipificados como tal y por consiguiente podrán ser juzgados por las autoridades competentes.

Se definen como delitos informáticos todas aquellas acciones ejecutadas dentro del espacio virtual que promueven un delito individual, social, económico y político. Estos delitos son de tres tipos: los delitos informáticos con fines económicos, los delitos informáticos sociales y los delitos informáticos políticos o ideológicos. En Colombia predominan los primeros, es decir los delitos informáticos que buscan la obtención de dinero.

Desde otro punto de vista, según la Instrucción 2/2011 dictada por la Fiscalía, los delitos informáticos se clasifican en tres bloques: 1) en los que el objeto de la actividad delictiva son las TIC, 2) en los que la actividad criminal se utiliza para tomar las ventajas que ofrecen las TIC, 3) en los que la actividad criminal, requiere de las ventajas que brindan las TIC, que en el fondo es compleja y que requiere conocimientos específicos en la materia.

También, los delitos informáticos más comunes cometidos a través de Internet o de las TIC y que son de interés para este trabajo son los siguientes: 1) contra la intimidad: ataques a sistemas informáticos o su interceptación, 2) contra el patrimonio y orden social y económico en el que se descubre información empresarial sensible, se generan daños informáticos o sabotaje, delitos contra servicios de radiodifusión o interactivos.

Aunque el uso de Internet y la implementación general de las TIC no está extendida en toda Colombia todavía, la transformación digital del país es un hecho, y trae un aumento en los riesgos de seguridad digital, pues cada vez más se utilizan las herramientas tecnológicas y hay aumento de denuncias de delitos informáticos.

Para el desarrollo del presente documento se establecieron tres objetivos específicos que permiten alcanzar el cumplimiento del objetivo general, de los cuales se obtuvieron los siguientes resultados:

- Se define qué es el medio informático y se presentan las potenciales modalidades de delitos informáticos en Colombia.
- Se establecieron cuáles son las medidas de seguridad informática en Colombia y cuáles son las sanciones aplicadas a quien incurren en estas conductas delictivas y quebrantan estas normas que buscan contrarrestar el delito de hurto informático.

- Se presenta un análisis de la evolución de los delitos informáticos de cara al actual marco legislativo internacional y la Ley 1273 de 2009 de Colombia y se corrobora que está vigente esta normatividad a pesar de que la tecnología evoluciona rápidamente. Lo que habría que incluir en esta ley sería la regulación del ciberespacio como también interponer ciertas restricciones en el uso de este. Por lo cual los expertos han propuesto la creación de un tribunal internacional que tendría la facultad de enjuiciar individualmente a las personas que cometen los delitos cibernéticos más graves de trascendencia e interés global.
- Hay grupos delictivos organizados, nacionales e internacionales, que cometen delitos informáticos, que en algunos casos son contrarrestados por la seguridad informática, pero que en la gran mayoría de las veces es imposible capturar a quienes los cometen, pues lo hacen a distancia y los llevan a cabo de forma rápida y sin dejar huella.
- A partir del estudio realizado en este trabajo, se puede concluir que en el país se cuenta con la Ley 1273 que permite sancionar los delitos informáticos. Se entiende por delito informático todas aquellas acciones ilegales que se cometen mediante el uso de la informática y el Internet. No hay que confundir los delitos comunes realizados mediante Internet y/o con un computador, de los ciberdelitos, como se ha explicado en este estudio.

10. Conclusiones

Los delitos informáticos en Colombia se rigen en materia penal por medio de la Ley 1273 de 2009, conocida como ley de delitos informáticos. Esta norma tiene como fin castigar jurídicamente a los ciberdelincuentes que cometan este tipo de delitos, allí se encuentran descritos y tipificados como tal y por consiguiente podrán ser juzgados por las autoridades competentes. Los delitos informáticos en Colombia tienen la sanción económica más alta del Código Penal; la más baja es de 100 salarios mínimos legales vigentes, mientras que la máxima puede ser de 1.000 salarios mínimos legales vigentes. Asimismo, se castigará a los delincuentes con pena de prisión de 48 a 96 meses, dependiendo del delito en el cual se haya incurrido.

En el capítulo primero de la mencionada ley hay referencia a los siguientes delitos: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, daño informático, uso de *software* malicioso, interceptación de datos informáticos, suplantación de sitios web para capturar datos personales y violación de datos personales. La Ley 1273 de 2009 se fundamenta en el convenio internacional de Budapest, por lo cual tiene plena vigencia y abarca todas las modalidades de delitos informáticos. Para cada delito hay estipuladas una sanción económica y una pena de prisión.

En este trabajo se consideran como delitos informáticos todas aquellas acciones ejecutadas dentro del espacio virtual que promueven un crimen individual, social, económico y político, que ha sido contemplado en el orden jurídico nacional en el que alguna de las partes implicadas se encuentre, tanto víctimas como victimarios. Asimismo, los delitos informáticos son todas aquellas actividades delictivas que se ejecutan mediante el uso de computadores. También es delito atentar contra un sistema informático y la información que este contiene. Como se dijo, los delitos

informáticos son de tres tipos: los delitos informáticos con fines económicos, los delitos informáticos sociales y los delitos informáticos políticos o ideológicos.

En cuanto al hurto informático, las autoridades tienen un gran reto para contrarrestar este delito, siendo un hecho punible que atenta contra la seguridad de los ciudadanos, debido a que la acción de hurtar por este medio implica poner en riesgo la integridad de las personas y la seguridad de las empresas, pues este tipo de hurto se comete con fines económicos ya que quien comete el hecho delictivo obtiene un beneficio propio o para un tercero de común acuerdo.

Las entidades jurídicas del Estado colombiano deben tener la suficiente capacitación en seguridad informática y las tecnologías adecuadas. Aunque el Estado colombiano ha hecho considerables inversiones en este aspecto, todavía falta esfuerzos para avanzar en seguridad informática. Se debe contratar personal capacitado y calificado para el manejo de la información, los *insiders* deben ser personas altamente confiables porque son quienes manejan la información de las empresas; también se debe hacer un estudio riguroso para seleccionar a las personas adecuadas para proteger la información de los ciudadanos y los datos que puedan ser vulnerados por los delincuentes informáticos.

Además, los funcionarios judiciales, en especial algunos fiscales y jueces, deben tener experiencia relacionada en conocimientos de delitos informáticos, específicamente en el delito de hurto informático, y lo que representa el daño al bien jurídico tutelado que se conoce como “ de la protección de la información y de los datos”, como la protección íntegra de las tecnologías de la información del Estado colombiano como nuevo tipo penal que ampara el derecho a la protección de la información, garantía constitucional que se encuentra en los Artículos 15 y 20 de la Constitución Política de Colombia de 1991.

Dicha ley castiga fuertemente el acceso abusivo a los sistemas informáticos y la obstaculización ilegal del sistema informático o redes de telecomunicaciones con una pena alta. Así las cosas, la persona que sin estar facultada impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos que allí hay, o a una red de telecomunicaciones, está incurriendo en delito.

Respecto a los ciberdelincuentes es el vínculo del territorio el que justifica la aplicación de la ley penal. Es decir, que la aplicación de la ley depende del país donde se haya cometido el delito.

Las penas se aumentarán más si el delito se comete sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. Y si el que comete el delito es un servidor público en ejercicio de sus funciones y abusa de la confianza depositada sobre quien posee la información.

El uso de los sistemas informáticos y las TIC son parte fundamental de la vida moderna y son imprescindibles en los ámbitos empresarial, personal, de salud, de comunicación y de bienestar de la sociedad; sin embargo, a la par con estos avances tecnológicos se desarrollan los denominados delitos informáticos que lesionan o causan daño a la sociedad y a la economía, por lo cual requieren una protección integral del Estado.

La transformación digital del país trae también un aumento en los riesgos de seguridad digital, pues cada vez más se utilizan las herramientas tecnológicas. Por lo tanto, la seguridad informática es indispensable en las entidades para afrontar las amenazas del entorno cibernético. Se requiere la preparación del personal de las empresas, los directivos de las entidades deben designar recursos adecuados para asegurar la protección frente a las cibernéticas.

Los delitos informáticos se deben afrontar desde la interdisciplinariedad pues tanto ingenieros de sistemas como juristas, deben trabajar en pro de la seguridad y la salvaguarda de la información y de los datos de las empresas y personas. De hecho, la investigación realizada por Ojeda et al. (2010) fue realizada por un equipo interdisciplinar compuesto por un ingeniero de sistemas, un abogado, un ingeniero de telecomunicaciones y un economista.

Por último, hay que destacar que toda la terminología de los delitos informáticos viene en el idioma inglés, que es la lengua a través de la cual se difunde la ciencia y la tecnología, lo cual hace difícil comprender las amenazas a las que nos vemos enfrentados. Los siguientes términos son ejemplos de esto: *cracker, computer crime, cybersecurity*, *hackers*, *insider, malware, phishing, ransomware*, *smishing, spyware* y *vishing*, entre otros. Sería recomendable utilizar siempre estas palabras y expresiones en español.

Referencias Bibliográficas

Abushihab, M. (2016). *Hurto por medios informáticos. ¿Un delito informático?* . Universidad Santo Tomás.

Barrios, S. (2012). *El delito informático en la legislación colombiana* . Corporación Universitaria de la Costa, CUC.

Barrios, V., & Vargas, A. (2018). *Convenio sobre la ciberdelincuencia: Convenio de Budapest.* Biblioteca del Congreso Nacional de Chile [BCN].

Cadena, A. (2021). *Crecimiento del ciberfraude en Colombia durante la pandemia por covid-19* . Universidad Militar Nueva Granada.

Cámara Colombiana de Informática y Telecomunicaciones. (2019). *Tendencias del cibercrimen en Colombia.*

Carriedo, L. M. (2022). *Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México* . Infotec.

Congreso de la República . (1991). *Constitución Política de Colombia* . Diario Oficial.

Congreso de la República . (2000). *Ley 599 de 2000. Código Penal.* República de Colombia.

Congreso de la República. (2009). *Ley 1273 de 2009.* Diario Oficial .

Congreso de la República de Colombia. (2009). *Ley 1341 de 2009.* República de Colombia.

Corte Constitucional [CC]. (2011). *M. P.: J. I. Pretelt. Sentencia C-748/11.* (Colombia). Obtenido el 9 de agosto de 2022.

Corte Constitucional [CC]. (2019). *M. P.: C. Bernal y A. Fajardo. Sentencia T-039/19.* (Colombia). Obtenido el 5 marzo de 2019.

Corte Constitucional [CC]. (2019). *M. P.: C. Schlesinger. Sentencia C-224.* (Colombia). Obtenido el 27 de mayo de 2022.

Corte Constitucional [CC]. (2020). *M. P.: A. Linares Cantillo. Sentencia C-094/20.* (Colombia). Obtenido el 9 de agosto de 2022.

Corte Suprema de Justicia [CSJ]. (2015). *Sala de Casación Penal, julio 24, 2015. M. P.: E. Patiño. Sentencia SP-1245/15.* (Colombia). Obtenido el 30 de julio de 2022.

Costas, S. J. (2011). *Seguridad informática. https://books.google.com.co/books?id=7I6fDwAAQBAJ&pg=PA17&hl=es&source=gbs_toc_r&cad=3#v=onepage&q&f=false.* Google books.

Devia, W., & Martínez, M. (2019). *Análisis del aumento en el hurto informático en el departamento de Córdoba durante los años 2015 y 2016.* Universidad Nacional Abierta y a Distancia.

El Tiempo. (2022). *Solo el 61,6 % de los hogares en Colombia tienen internet.*

Gómez, M. (2014). *Ciber Criminalidad: nuevos retos para la seguridad pública.* Universidad De Sonora.

Granados, R., & Parra, A. (2016). *El delito de hurto por medios informáticos que tipifica el artículo 269i de la Ley 1273 de 2009 y su aplicabilidad en el Distrito Judicial de Cúcuta en el período 2012 -2014* . Universidad Libre de Colombia.

Grisales, G. (2013). *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* . Universidad Eafit.

Guarnizo, M. P. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia* . Universidad Nacional Abierta y a Distancia.

Hernández, D. L. (2009). El delito informático. *Eguzkilore, 23*. https://doi.org/https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Informe SAFE. (2022). *Tendencias del cibercrimen 2021-2022.*

Jiménez, A., & Milagros, R. (2019). *El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima.* Universidad César Vallejo.

Jiménez, A., & Milagros, R. (2020). *El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019* . Universidad César Vallejo.

Ministerio de Tecnologías de la Información y de las Comunicaciones. (2019). Aspectos básicos de la industria 4.0.: https://colombiatic.mintic.gov.co/679/articles-124767_recurso_1.pdf

Núñez, E. (2021). *Metodología para la detención y reducción de Rasomware.* Trabajo de grado, Universidad Nacional de Piura. https://doi.org/https://repository.ugc.edu.co/bitstream/handle/11396/2377/Guia_APA_interactiva_vol2%20%282%29%20%281%

Ojeda-Pérez, J., Rincón-Rodríguez, F., Arias-Flórez, M., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11*(28), 41-66. https://doi.org/https://revistas.javeriana.edu.co/index.php/cuacont/article

Osorio, C. (2022). *Ataques informáticos. La precaria ciberseguridad de Colombia.* El País.

Palomá, L. O. (2012). *Delitos informáticos (en el ciberespacio) doctrina y análisis de casos reales.* Ediciones Jurídicas Andrés Morales.

Portafolio. (12 de julio de 2022). *Más de 29.000 ciberdelitos se han denunciado en 2022*.

Rivera, M. (2020). *La tentativa en el delito de hurto mediante medios informáticos.* Universidad Externado de Colombia.

Sánchez, D. (2022). *Impacto de la pandemia covid-19 en la protección de datos en Colombia.* Universidad Santo Tomás.

Torres, H. (2013). *La delincuencia organizada transnacional en Colombia* .

Torres-Torres, H. W. (2022). *Derecho informático.* Ediciones Jurídicas.

Valencia, B. M., Puerta, B. J., Collazos, B. N., Urrea, D., & Cañas, C. (2019). Influencia de la cuarta revolución industrial en Colombia. *Punto de Vista , 10*(16), 1-19.

Ventura, M. (. (2020). *La tipificación del Phishing, Smishing y Vishinhg en nuestro sistema penal peruano, para la lucha conta la ciberdelincuencia en Lima* . Trabajo de grado, Universidad privada del Norte.